MAXIMUS

Managed Risk Medical Insurance Board
Contract 02MHF026
Report on Controls in Operation
and
Tests of Operating Effectiveness
February 28, 2009

REPORT ON CONTROLS IN OPERATION AND TESTS OF
OPERATING EFFECTIVENESS
February 28, 2009

TABLE OF CONTENTS

SECTION	PAGE

SECTION ONE

Independent Service Auditor's Report

SECTION ONE – INDEPENDENT SERVICE AUDITOR'S REPORT

Mr. Bruce Caswell, President, MAXIMUS Operations Group

We have examined the accompanying description of controls related to MAXIMUS in connection with your contract 02MHF026 with the State of California Managed Risk Medical Insurance Board (MRMIB) related to the California Healthy Families program and the Access for Infants and Mothers program (the Programs). Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of MAXIMUS's controls that may be relevant to the MRMIB's internal control as it relates to the Programs; (2) the controls included in the description were suitably designed to achieve the control objectives specified in the description, if those controls were complied with satisfactorily and the MRMIB applied the controls contemplated in the design of MAXIMUS's controls; and (3) such controls had been placed in operation as of February 28, 2009. The control objectives were specified by the management of MAXIMUS. Our examination was performed in accordance with standards established by the American Institute of Certified Public Accountants and included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

In our opinion, the accompanying description of the aforementioned controls presents fairly, in all material respects, the relevant aspects of MAXIMUS's controls in connection with contract 02MHF026 with the MRMIB related to the Programs that had been placed in operation as of February 28, 2009. Also, in our opinion, the controls, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily and the MRMIB applied the controls contemplated in the design of MAXIMUS's controls.

In addition to the procedures we considered necessary to render our opinion as expressed in the previous paragraph, we applied tests to specific controls, which are presented in Section Three of this report, to obtain evidence about their effectiveness in meeting the related control objectives described in Section Three, during the period from March 1, 2008 to February 28, 2009. The specific controls and the nature, timing, extent, and results of the tests are listed in Section Three. This information has been provided to the MRMIB and to their auditors to be taken into consideration, along with information about the internal control at the MRMIB, when making assessments of control risk for MRMIB. In our opinion the controls that were tested, as described in Section Three, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in Section Three were achieved during the period from March 1, 2008 to February 28, 2009.

The relative effectiveness and significance of specific controls at MAXIMUS in connection with contract 02MHF026 with the MRMIB related to the Programs and their effect on assessments of control risk at the MRMIB are dependent on their interaction with the controls and other factors present at the MRMIB. We have performed no procedures to evaluate the effectiveness of controls at the MRMIB.

The description of controls at MAXIMUS is as of February 28, 2009, and information about tests of the operating effectiveness of specific controls covers the period from March 1, 2008 to February 28, 2009. Any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the controls in existence. The potential effectiveness of specific controls at MAXIMUS in connection with contract 02MHF026 with the MRMIB related to the Programs is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the system or controls, (2) changes in processing requirements, or (3) changes required because of the passage of time, may alter the validity of such conclusions.

This report is intended solely for use by the management of MAXIMUS, the State of California Managed Risk Medical Insurance Board (MRMIB), and the auditors of the State of California.

Lurie Besikof Lapidus & Company, LLP

Lurie Besikof Lapidus & Company, LLP
May 13, 2009

SECTION TWO

Description of Controls Provided by MAXIMUS

SECTION TWO – DESCRIPTION OF CONTROLS PROVIDED BY MAXIMUS

Scope of this Report

This report was prepared in accordance with the guidance contained in the American Institute of Certified Public Accountants' Statement on Auditing Standards (SAS) No. 70, "Service Organizations," its amendments and interpretations. This report only encompasses aspects of the services provided or procedures followed by MAXIMUS under their contract number 02MHF026 with the State of California's Managed Risk Medical Insurance Board (MRMIB) related to the California Healthy Families program and the Access for Infants and Mothers program (the Programs).

The description provided by MAXIMUS in Section Two only address the controls related to the processing of transactions under their contract number 02MHF026 with the MRMIB related to the Programs. MAXIMUS has specified its control objectives relating to the processing of transactions under its contract number 02MHF026 with the MRMIB related to the Programs. For each control objective, MAXIMUS has indicated controls that are designed to achieve the stated control objective. Information on the nature, timing, and extent of testing conducted by MAXIMUS's independent service auditor, Lurie Besikof Lapidus & Company, LLP (Service Auditor), is provided in Section Three of this report. Unless noted as "Results of Tests" in the "Testing Performed by the Service Auditor" section, there were no significant exceptions in the testing considered to be relevant to the auditors of the MRMIB.

MAXIMUS, Administrative Contractor for the California Healthy Families Program

The administration and computer functions for the MRMIB for the MAXIMUS California Healthy Families program and the Access for Infants and Mothers program are located in California.

The California Healthy Families program is the California implementation of the Federal State Children's Health Insurance Program (SCHIP), Title XXI Act. The Access for Infants and Mothers program is low-cost health coverage for pregnant women and their newborns implemented by Title 10 of the California Code of Regulations, Chapter 5.6. The MRMIB contracted with MAXIMUS to act as the Administrative Contractor for the Programs. MAXIMUS, as the Administrative Contractor, is required to perform the administrative functions including the maintenance of case records, invoicing for health care premiums, collection of premiums, and the maintenance of financial records for the Programs under the direction of the MRMIB.

MAXIMUS's administrative functions under the contract with the MRMIB for the Programs include data systems supporting fully integrated eligibility, enrollment and financial/accounting systems.

maintains all training records.

Control Activities

Risk Assessment

MAXIMUS (Organization) has placed into operation a risk assessment process to identify and manage risks that could affect the Organization's ability to provide reliable transaction processing for user organization, the MRMIB. This process requires management to identify significant risks in their areas of responsibility and to implement appropriate measures to address those risks. This process has identified risks resulting from the nature of the services the Organization provides, and management has implemented various measures to manage those risks.

Monitoring

The Organization's management and supervisory personnel monitor the quality of internal control performance as a routine part of their activities.

Fraud Prevention and Detection

Assurance that the potential for fraud (unauthorized access to the Organization or participant data) is adequately monitored, mitigated and detected is achieved through segregation of duties and strict adherence to rules, information security policies and practices, and procedures described in this report. Additional assurance is provided by external audits of controls and reconciliation activities.

Information and Communications

Information Systems

Multiple servers and databases support numerous processes from application processing to financial posting.

Controls Overview

Description of Information Systems General Controls

Control Objective 1: Controls provide reasonable assurance that Project Management demonstrates, through attitude, awareness and actions, an atmosphere that enhances the effectiveness of specific policies and procedures. Controls provide reasonable assurance that the Organization structure provides appropriate division of responsibilities. Controls provide reasonable assurance that service levels are defined and managed in a manner that satisfies case management system requirements and provides a common understanding of performance levels with which the quality of services are measured. Controls provide reasonable assurance that third-party services are secure, accurate and available, support processing integrity and defined appropriately in performance contracts.

Project Oversight Strategy

1. Management has mechanisms to obtain feedback from relevant external stakeholders, business process owners, and end-users regarding the quality and usefulness of IT and IS.

2. The Project's Management monitors its progress against planned performance measures and reacts accordingly to meet established objectives.

Organization and Relationships

3. Directors, managers and technicians have adequate knowledge and experience to fulfill their responsibilities.

4. Key systems and data have been inventoried and their owners identified.

5. Roles and responsibilities of the Organization are defined, documented and understood.

6. Personnel have sufficient authority to exercise the role and responsibility assigned to them.

7. Personnel understand and accept their responsibility regarding internal control.

8. Management has implemented a division of roles and responsibilities (segregation of duties) that reasonably prevent a single individual from subverting a critical process.

9. Staff evaluations are performed regularly (e.g., ensure the IT function has a sufficient number of competent IT staff necessary to achieve objectives). Employees receive their first written performance evaluation after 90 days of employment.

10. Contracted staff and other contract personnel are subject to policies and procedures created by the IT function to control their activities and to assure the protection of the Project's information assets.

11. Significant IT events or failures, e.g., security breaches, major system failures or regulatory failures, are reported to senior management.

Management of Human Resources

12. Controls are in place to support appropriate and timely responses to job changes and job terminations so that internal controls and security are not impaired by such occurrences.

Educate and Train Users

13. The Project subscribes to a philosophy of continuous learning, and providing necessary training and skill development to its members.

14. Established procedures for identifying and documenting the training needs of all personnel that use information services in support of the Project exist.

15. Management provides education and ongoing training programs that include ethical conduct, system security practices, confidentiality standards, integrity standards, and security responsibilities for all staff.

Assessment of Risks

16. The Project has an activity-level risk assessment framework, which is used periodically, to assess information risk for achieving business objectives and considers the probability and likelihood of threats.

Manage Facilities

21. Facilities are adequately secured and managed.

22. Data center facilities are equipped with adequate environmental controls to maintain systems and data, including fire suppression, uninterrupted power service (UPS), generator, and appropriate air conditioning.

Compliance with External Requirements

23. Control activities are in place and followed to ensure compliance with external requirements, such as regulatory and legal rules.

24. Internal events are considered in a timely manner to support continuous compliance with legal and regulatory requirements.

Management of Quality

25. Documentation is created and maintained for all significant processes, controls and activities.

26. A plan to maintain the overall quality assurance of activities, based on the Project plans, exists.

27. Documentation standards are in place, have been communicated to all staff, and are supported with training.

28. A quality plan exists for significant IT functions (e.g., large system development and deployment projects) and provides a consistent approach to address both general and project-specific quality assurance activities.

29. The quality plan prescribes the type(s) of quality assurance activities (such as reviews, audits, inspections) to be performed to achieve the objectives of the quality plan.

30. The quality assurance process includes a review of adherence to policies, procedures and standards.

Manage Performance and Capacity

31. IT management monitors the performance and capacity levels of the systems and network.

32. IT management has a process in place to respond to suboptimal performance and capacity measures.

33. Performance and capacity planning is included in system design and implementation activities.

Monitoring

34. Performance indicators or benchmarks, from both internal and external sources, have been defined, and data is collected and reported regarding achievement of these benchmarks.

35. Management has established appropriate metrics to effectively manage the day-to-day activities.

36. Management monitors delivery of services to identify shortfalls and responds with actionable plans to improve.

Adequacy of Internal Control

37. Management monitors the effectiveness of internal controls in the normal course of operations through management and supervisory activities, comparisons and benchmarks.

38. Serious deviations in the operation of internal control, including major security, availability and processing integrity events, are reported to senior management.

39. Internal control assessments are performed periodically, using self-assessments, to examine whether or not internal controls are operating satisfactorily.

Internal Audit

40. Internal Audit engagements are performed based on approval by the audit committee.

Third-Party Services

41. A designated individual is responsible for regular monitoring and reporting on the achievement of the third-party service level performance criteria.

42. The selection of vendors for outsourced services is performed in accordance with the Project's vendor management policy.

43. Before selection, management determines that potential third parties are properly qualified through an assessment of their capability to deliver the required service.

44. Third-party service contracts address the risks, security controls and procedures for information systems and networks in the contract between the parties.

45. Procedures exist and are followed to ensure that a formal contract is defined and agreed to for all third-party services before work is initiated, including definition of internal control requirements and acceptance of the Project's policies and procedures.

46. A regular review of security, availability and processing integrity is performed for service level agreements and related contracts with third-party service providers.

Description of Computer Operations Controls

General Operations

Control Objective 2: Controls provide reasonable assurance that any problems and/or incidents are properly responded to, recorded, resolved, or investigated for proper resolution.

Control Objective 3: Controls provide reasonable assurance that data recorded, processed and reported remains complete, accurate and valid throughout the update and storage process.

Control Objective 4: Controls provide reasonable assurance that authorized programs are executed as planned and deviations from scheduled processing are identified and investigated.

Security and Access

Control Objective 5: Controls provide reasonable assurance that Project IT operating systems and subsystems are appropriately secured to prevent unauthorized use, disclosure, modification, damage, or loss of data.

Control Objective 6: Controls provide reasonable assurance that all IT components, as they relate to security, processing and availability, are well protected, would prevent any unauthorized changes, and assist in the verification and recording of the current configuration.

Acquisition, Development and Change

Control Objective 7: Controls provide reasonable assurance that technology infrastructure is acquired so that it provides the appropriate platforms to support case management operating applications.

Control Objective 8: Controls provide reasonable assurance that application software is acquired or developed to effectively support case management operating requirements.

Control Objective 9: Controls provide reasonable assurance that systems are appropriately tested and validated prior to being placed into production processes, and that associated controls operate as intended and support case management operating requirements.

Control Objective 10: Controls provide reasonable assurance that policies and procedures defining required acquisition and maintenance processes have been developed and are maintained, and that they define the documentation needed to support the proper use of the applications and the technological solutions put in place.

Control Objective 11: Controls provide reasonable assurance that system changes of operational significance are appropriately tested and authorized before movement into production.

Description of Application Controls – Input, Processing and Output

Input Controls

Control Objective 12: Input controls provide reasonable assurance.

Processing Controls

Control Objective 13: Processing controls provide reasonable assurance.

Output Controls

Control Objective 14: Output controls provide reasonable assurance.

Description of Systems Application Processing Controls – Financial Management Systems

Input Controls

Control Objective 15: Input controls provide reasonable assurance that:

- Originating HFP and AIM source data are entered by trained and authorized persons, and data preparation procedures are established and followed to minimize errors and omissions, and to allow the input of only valid data into the system.

- Authorized source documentation and data is complete and accurate, properly accounted, and transmitted in a timely manner.

- Error handling procedures detect errors and irregularities and report them for corrective action.

- Source documents are retained and available for reconstruction and legal compliance.

Processing Controls

Control Objective 16: Processing controls provide reasonable assurance that:

- Data is posted to the correct files, completely and accurately.

- Unauthorized changes to data are prevented.

- Database files remain complete and accurate until changes occur as a result of authorized processing.

- Procedures assure that balancing of data is made with relevant control totals. Transaction processing can be traced effectively to reconcile disrupted data.

- Continued integrity of stored data.

- Procedures establish development standards, as appropriate, for electronic transaction integrity and authenticity (atomicity, consistency, isolation, and durability).

Output Controls

Control Objective 17: Output controls provide reasonable assurance that:

- Procedures define handling and retention of output. When negotiable instruments are produced, special care is taken to prevent misuse.

- Procedures define and assure appropriate distribution of IT output.

- Procedures are communicated for physical and logical access to output. Confidentiality of output is defined and taken into consideration in the procedures.

- Procedures assure that both provider and user review output for accuracy and that procedures control errors contained in output.

- Physical access to output printers and subsequent storage areas is restricted to authorized personnel.

User Control Considerations

The MAXIMUS California Healthy Families and Access for Infants and Mothers projects controls were designed with the assumption that certain controls would be implemented by the user organization, the MRMIB. In certain situations, the application of specific controls at the MRMIB is necessary to achieve certain control objectives included in this report.

This section describes additional controls that should be in operation at the MRMIB to complement the controls at the MAXIMUS California Healthy Families and Access for Infants and Mothers projects. The MRMIB and its user auditors should consider whether the following controls have been placed in operation at the MRMIB:

- Controls to provide reasonable assurance that output reports are reviewed by appropriate individuals at the MRMIB for completeness and accuracy

- Controls to provide reasonable assurance that output received from the MAXIMUS projects is routinely reconciled to relevant MRMIB data and other control totals

- Controls to provide that daily cash sweeps from the MAXIMUS Projects cash accounts are appropriately reconciled to the corresponding daily deposits in the State's accounts

The above list of user control considerations do not represent a comprehensive set of all the controls that should be employed by the MRMIB. Other controls may be required at the MRMIB.

SECTION THREE

Information Provided by the Service Auditor

SECTION THREE – INFORMATION PROVIDED BY THE SERVICE AUDITOR

Overview of Control Objectives, Related Controls, and Tests of Operating Effectiveness

This report is intended to provide interested parties with information about the MAXIMUS controls in connection with its contract 02MHF026 with the MRMIB related to the California Healthy Families program and the Access for Infants and Mothers program (the Programs), and to provide information about the operating effectiveness of controls that were tested. This report, when combined with an understanding and assessment of the internal controls at the user organization, the MRMIB, is intended to assist the user organization's auditors in planning the audit of the user's financial statements and in assessing control risk for assertions in the user's financial statements that may be affected by controls at MAXIMUS in connection with contract 02MHF026 with the MRMIB related to the Programs.

Our testing of the controls related to MAXIMUS in connection with its contract 02MHF026 with the MRMIB related to the Programs was performed in Folsom, California. Our testing was restricted to the control objectives and the related controls listed beginning on page 11 in the "Controls Overview" section and on the following pages, and was not extended to procedures that may be in effect at the user organization, the MRMIB.

It is the user organization auditor's responsibility to evaluate this information in relation to the controls in place at the user organization. If certain complementary controls are not in place at the user organization, MAXIMUS's controls in connection with contract 02MHF026 with the MRMIB related to the Programs may not compensate for such weaknesses.

Our examination considered the control environment and included inquiry of appropriate management, supervisory and staff personnel, inspection of documents and records, observation of activities and operations, and tests of controls surrounding and provided by MAXIMUS's processing in connection with its contract 02MHF026 with the MRMIB related to the Programs. Our tests of controls covered the period March 1, 2008 to February 28, 2009, and were applied to those controls relating to control objectives specified by MAXIMUS.

The description of control objectives and controls are the responsibility of MAXIMUS management. Lurie Besikof Lapidus & Company, LLP's responsibility is to express an opinion that the controls are operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives, specified by MAXIMUS management, were achieved during the period covered by this report.

MAXIMUS developed an application specific to the needs of the California Healthy Families program and the Access for Infants and Mothers program. The application was developed in the MAXIMUS proprietary development system. The financial application support used by MAXIMUS in connection with its administrative duties for the Programs is provided by Oracle Financials. The system provides the front end support for the Oracle Financials application providing various billing information to the Oracle Financials application. Oracle Financials provides Accounts Receivable, General Ledger, and Accounts Payable functionality. Oracle Financials provides collection delinquency information back to the system for follow-up and if necessary disenrollment in the Programs. For the purpose of this report, the application specific to the needs of the California Healthy Families program and the Access for Infants and Mothers program will be referred to as the system, the MAXIMUS administration of the Programs will be referred to as the Project, and Oracle Financials will be referred to specifically.

The description of the tests of operating effectiveness and the results of those tests detailed on the following pages are the responsibility of Lurie Besikof Lapidus & Company, LLP.

General Description of Testing Procedures Performed

Tests performed of the operational effectiveness of controls are described in general below and in more detail on the following pages:

Type of Test	General Description of Test
Corroborative inquiry, inquiry, or discussion	Made inquiries of appropriate personnel and corroborated responses with other personnel to ascertain compliance with controls.
Observation	Observed application of specific controls.
Inspected, obtained and inspected	(Obtained and) inspected documents and/or reports indicating performance of the controls.
Reviewed, obtained and reviewed	Reviewed documents and reports indicating performance of the controls.
Compared	Compared information obtained from two independent sources to confirm the operation of the control.
Selected, selected and reviewed	Randomly selected records from a population and reviewed for compliance with controls.
Verified	Confirmed the controls were functional.
Tested	Re-performed application of the controls.

Control Objectives, Control Activities, Testing Performed, and Results of Tests

I. Information Systems General Controls		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
Control Objective 1: Controls provide reasonable assurance that Project Management demonstrates, through attitude, awareness and actions, an atmosphere that enhances the effectiveness of specific policies and procedures. Controls provide reasonable assurance that the Organization structure provides appropriate division of responsibilities. Controls provide reasonable assurance that service levels are defined and managed in a manner that satisfies case management system requirements and provides a common understanding of performance levels with which the quality of services are measured. Controls provide reasonable assurance that third-party services are secure, accurate and available, support processing integrity and defined appropriately in performance contracts.		
Project Oversight Strategy		
1. Management has mechanisms to obtain feedback from relevant external stakeholders, business process owners, and end-users regarding the quality and usefulness of IT and IS.	• *Obtained and reviewed* the following: ▪ Bi-Weekly MRMIB Progress Meeting minutes ▪ Weekly Tactical Meeting minutes ▪ Internal Policy Work Group (IPWG) minutes ▪ DHS and the MRMIB Bi-Weekly Coordination Meeting minutes	No relevant exceptions were noted. The information reviewed confirms management's description. Noted that the minutes contained discussion around the input from various stakeholders, business process owners, and end-users regarding: • Risk reporting • Personnel reporting • Open alerts and Key Performance Review (KPR) status • Problem Correction System (PCS) aging reporting • Change Action Requests (CARs), • Programs updates.
	• *Inquired* of selected Programs personnel to determine policies.	No relevant exceptions were noted. The inquiries confirm management's description.

I. Information Systems General Controls

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test

2. The Project's Management monitors its progress against planned performance measures and reacts accordingly to meet established objectives.	• *Obtained* and *reviewed* the following:
	  ▪ Weekly Tactical Meeting minutes
	  ▪ California Healthy Families Program (CAHFP) Performance Standards spreadsheet.
		No relevant exceptions were noted. The information reviewed confirms management's description.

	• *Inquired* of the Director of the Project / Program regarding the weekly staff meetings containing the agenda item reviewing the key metrics.	No relevant exceptions were noted. The inquiries confirm management's description.
	• *Traced* a sample of the CAHFP Performance Indicators spreadsheet to the source documents verifying that the source data agreed to the measurement presented in the spreadsheet.	No relevant exceptions were noted. A statistically valid sample of fourteen (14) performance indicators was selected for tracing to the source documents. The tests performed confirm management's description.

I. Information Systems General Controls		
Controls Specified by MAXIMUS	**Testing Performed by the Service Auditor**	**Results of Test**
Organization and Relationships		
3. Directors, managers and technicians have adequate knowledge and experience to fulfill their responsibilities.	• *Inspected* the job descriptions for the following positions: ■ Business Analyst ■ Health Systems Analyst ■ Application Developer ■ Database Administrator ■ Lead Applications Developer ■ Senior Application Developer ■ Senior Oracle Financial Developer ■ Senior Web Developer ■ IS Management Team ■ Quality Assurance Job Descriptions ■ Project Director and Deputy Project Manager	No relevant exceptions were noted. The documents inspected confirm management's description.
	• *Inspected* the training curriculum for new hires and continuing education.	No relevant exceptions were noted. The documents inspected confirm management's description.
	• *Traced* a sample of employees to passing exam scores for training classes that culminate with an assessment or test where a test is required by the Project.	No relevant exceptions were noted. A statistically valid sample of twenty-eight (28) employees was selected for tracing to the passing exam scores contained in their HR files. The tests performed confirm management's description.

I. Information Systems General Controls		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
4. Key systems and data have been inventoried and their owners identified.	• *Inspected* the Organization chart and job descriptions.	No relevant exceptions were noted. The documents inspected confirm management's description.
	• *Inspected* appropriate information systems documentation indicating key systems and their owners.	No relevant exceptions were noted. The documents inspected confirm management's description.
	• *Inquired* of the Technical Infrastructure Manager and the Finance Director as to the process of inventorying and identifying system owners.	No relevant exceptions were noted. The inquiries confirm management's description.

I. Information Systems General Controls		
Controls Specified by MAXIMUS	**Testing Performed by the Service Auditor**	**Results of Test**

5. Roles and responsibilities of the Organization are defined, documented and understood.	• *Inspected* the following:
	  ▪ Organization chart
	  ▪ Job descriptions
	  ▪ New hire orientation training records
	
	• *Inspected* the job descriptions for the following positions:
	  ▪ Business Analyst
	  ▪ Health Systems Analyst
	  ▪ Application Developer
	  ▪ Database Administrator
	  ▪ Lead Applications Developer
	  ▪ Senior Application Developer
	  ▪ Senior Oracle Financial Developer
	  ▪ Senior Web Developer
	  ▪ IS Management Team
	  ▪ Quality Assurance Job Descriptions
	  ▪ Project Director and Deputy Project Manager.
		No relevant exceptions were noted. The documents inspected confirm management's description.
		Noted that the responsibilities are defined by organizational structure and hiring documentation combined with the job descriptions.
		
		No relevant exceptions were noted. The documents inspected confirm management's description.
		Noted that the responsibilities are defined in HR job descriptions combined with the organizational structure and hiring documentation.

I. Information Systems General Controls		
Controls Specified by MAXIMUS	**Testing Performed by the Service Auditor**	**Results of Test**
6. Personnel have sufficient authority to exercise the role and responsibility assigned to them.	• *Inspected* the following: ▪ Departmental Organization charts ▪ Job Descriptions	No relevant exceptions were noted. The documents inspected confirm management's description. Noted that the responsibilities are defined in HR job descriptions combined with the organizational structure & hiring documentation.
	• *Inquired* of several staff members as to the process noting conformity with stated policy.	No relevant exceptions were noted. The inquiries confirm management's description.
	• *Observed* staff members during the performance of their job duties.	No relevant exceptions were noted. The information reviewed confirms management's description.
	• *Inspected* the job descriptions for the following positions: ▪ Business Analyst ▪ Health Systems Analyst ▪ Application Developer ▪ Database Administrator ▪ Lead Applications Developer ▪ Senior Application Developer ▪ Senior Oracle Financial Developer ▪ Senior Web Developer ▪ IS Management Team ▪ Quality Assurance Job Descriptions ▪ Project Director and Deputy Project Manager.	No relevant exceptions were noted. The documents inspected confirm management's description.

I. Information Systems General Controls		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
7. Personnel understand and accept their responsibility regarding internal control.	• *Inspected* with the Director of Human Capital copies of signed Confidentiality Agreements and Statements of Privacy Practices for employees selected in a sample.	No relevant exceptions were noted. A statistically valid sample of sixty-four (64) employee files was selected for tracing to the signed Confidentiality Agreements contained in their HR files. The tests performed confirm management's description.
	• *Inquired* of several staff members as to their acceptance and responsibility regarding internal control.	No relevant exceptions were noted. The inquiries confirm management's description.
	• *Observed* staff during the performance of their job duties noting conformity with stated policy.	No relevant exceptions were noted. The procedures observed were consistent with management's description.

I. Information Systems General Controls

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
8. Management has implemented a division of roles and responsibilities (segregation of duties) that reasonably prevent a single individual from subverting a critical process.	• *Inspected* the Departmental Organization Charts and Job Descriptions noting segregation of duties.	No relevant exceptions were noted. The documents inspected confirm management's description.
	• *Observed* staff during the performance of their job duties noting conformity with stated policy.	No relevant exceptions were noted. The procedures observed were consistent with management's description.
	• *Inspected* the CAR process and procedures for the promotion of the code into production.	No relevant exceptions were noted. The documents inspected confirm management's description.
	• *Inquired* of the Manager of Software Engineering as to the process of promoting code into production noting conformity with stated policy.	No relevant exceptions were noted. The inquiries confirm management's description.
9. Staff evaluations are performed regularly (e.g., ensure the IT function has a sufficient number of competent IT staff necessary to achieve objectives).	• *Traced* a sample of employees to the performance evaluations contained in their HR files.	No relevant exceptions were noted. A statistically valid sample of sixty-four (64) employee files was selected for tracing to the performance evaluations contained in their HR files. The tests performed confirm management's description.
	• *Inquired* of the Director of Human Capital as to the procedures and methodology of the evaluations performed.	No relevant exceptions were noted. The inquiries confirm management's description.

I. Information Systems General Controls

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
10. Contracted staff and other contract personnel are subject to policies and procedures created by the IT function to control their activities and to assure the protection of the Project's information assets.	• *Inspected* a sample of the contracted staff's signed statements of privacy and practices.	No relevant exceptions were noted. A statistically valid sample of sixty-four (64) employee files was selected for tracing to the signed Confidentiality Agreements contained in their HR files. The tests performed confirm management's description.
	• *Inspected* new hire procedures documentation noting that it specifically states that it "pertains to: All contractors and temporary agencies staff."	No relevant exceptions were noted. The documents inspected confirm management's description.
	• *Inquired* of the Director of Human Capital meeting as to this procedure noting conformity with stated policy.	No relevant exceptions were noted. The inquiries confirm management's description.
11. Significant IT events or failures, e.g., security breaches, major system failures or regulatory failures, are reported to senior management.	• *Inspected* procedural documentation for security alerts and monitoring control noting conformity with stated policy.	No relevant exceptions were noted. The documents inspected confirm management's description.
	• *Inquired* of the Technical Infrastructure Manager as to the procedures followed for this policy.	No relevant exceptions were noted. The inquiries confirm management's description.
	• *Inspected* the system monitoring screens and online reporting.	No relevant exceptions were noted. The documents inspected confirm management's description.

I. Information Systems General Controls		
Controls Specified by MAXIMUS	**Testing Performed by the Service Auditor**	**Results of Test**
	• *Inspected* a copy of the Production Outage Report as of February 6, 2009, containing cumulative reporting of production outages since June 8, 2006.	No relevant exceptions were noted. The documents inspected confirm management's description.
Management of Human Resources		
12. Controls are in place to support appropriate and timely responses to job changes and job terminations so that internal controls and security are not impaired by such occurrences.	• *Inspected* Help Desk logs indicating job changes, additions and deletions.	No relevant exceptions were noted. The documents inspected confirm management's description.
	• *Tested* the system access lists by comparing to the current employee lists to determine if any terminated employees still have access.	No relevant exceptions were noted. The tests performed confirm management's description.
	• *Tested* the current application user IDs by comparing to the current employee lists to determine if any terminated employees still have access.	No relevant exceptions were noted. The tests performed confirm management's description.

I. Information Systems General Controls		
Controls Specified by MAXIMUS	**Testing Performed by the Service Auditor**	**Results of Test**
Educate and Train Users		
13. The Project subscribes to a philosophy of continuous learning, and providing necessary training and skill development to its members.	• *Inspected* a sample of the training records for selected staff noting continuous training throughout their employment history.	No relevant exceptions were noted. A statistically valid sample of twenty-eight (28) employees was selected noting continuous training throughout their employment history. The tests performed confirm management's description.
	• *Inquired* of the Training Supervisor as to this policy noting conformity with stated policy.	No relevant exceptions were noted. The inquiries confirm management's description.
	• *Inspected* training materials noting various education courses and materials.	No relevant exceptions were noted. The documents inspected confirm management's description.

I. Information Systems General Controls		
Controls Specified by MAXIMUS	**Testing Performed by the Service Auditor**	**Results of Test**
14. Established procedures for identifying and documenting the training needs of all personnel that use information services in support of the Project exist.	• *Inspected* a sample of the training records for selected staff noting procedures for identifying and documenting training needs of all personnel.	No relevant exceptions were noted. A statistically valid sample of twenty-eight (28) employees was selected noting procedures for identifying and documenting training needs. The tests performed confirm management's description.
	• *Inquired* of the Training Supervisor as to the policies and procedures in place noting conformity with stated policy.	No relevant exceptions were noted. The inquiries confirm management's description.
	• *Inspected* QMS documentation and training material for various education courses noting conformity with stated policy.	No relevant exceptions were noted. The documents inspected confirm management's description.
	• *Inspected* documentation of the security awareness training that all new staff is required to participate.	No relevant exceptions were noted. The documents inspected confirm management's description.
	• *Inspected* the employee manual and the Security and Confidentiality Policy for completeness noting conformity with stated policy.	No relevant exceptions were noted. The documents inspected confirm management's description.

I. Information Systems General Controls

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test

15. Management provides education and ongoing training programs that include ethical conduct, system security practices, confidentiality standards, integrity standards, and security responsibilities for all staff.	• *Reviewed* various QMS documents including but not limited to:
	  ▪ Security awareness training
	  ▪ Employee Manual
	  ▪ Security and Confidentiality Policy
	  ▪ New Hire Procedures
	  ▪ Training Needs Assessment
	  ▪ Training Database
	  ▪ Human Resources
	  ▪ SMUD Room Admittance
	  ▪ IS General Overview
		No relevant exceptions were noted. The information reviewed confirms management's description.

	• *Traced* a sample of employees to their respective training records for completeness.	No relevant exceptions were noted. A statistically valid sample of twenty-eight (28) employees was selected for tracing training records for completeness. The tests performed confirm management's description.
	• *Inquired* of the Training Supervisor and the training management as to the procedures concerning education and ongoing training programs.	No relevant exceptions were noted. The inquiries confirm management's description. Noted that all new employees are required to complete mandatory Corporate Compliance Courses within the first 5 days of employment. These include: MAXIMUS overview, sexual harassment prevention and workplace conduct, business ethics, information security awareness, privacy, and confidentiality.

I. Information Systems General Controls		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
Assessment of Risks		
16. The Project has an activity-level risk assessment framework that is used periodically to assess information risk for achieving business objectives and considers the probability and likelihood of threats.	• *Traced* a sample of the summary statistics (from the Key Performance Indicators report) to the source documents provided by the individual departments. • *Inspected* the monthly Risk Assessment reports discussed in the tactical meetings noting conformity with stated policy.	No relevant exceptions were noted. A sample of fourteen (14) individual summary statistics was selected for tracing to the source documents. The tests performed confirm management's description. No relevant exceptions were noted. The documents inspected confirm management's description.
17. A user access audit is performed for critical systems and locations based on their relative priority and importance to the Project on a weekly basis.	• *Inquired* of the Technical Infrastructure Manager as to the process of user audits noting conformity with stated policy. • *Compared* application user access rights to the current employee list for differences.	No relevant exceptions were noted. The inquiries confirm management's description. No relevant exceptions were noted. The tests performed confirm management's description.

I. Information Systems General Controls		
Controls Specified by MAXIMUS	**Testing Performed by the Service Auditor**	**Results of Test**
18. Where risks are considered acceptable, there is formal documentation and acceptance of residual risk with related offsets, including adequate insurance coverage, contractually negotiated liabilities and self-insurance.	• *Inquired* of the Contract Manager as to documentation of acceptable risk. • *Obtained and reviewed* the administrative contract with the MRMIB.	No relevant exceptions were noted. The inquiries confirm management's description. Noted that all vendors are covered under subservice contract agreements according to the MAXIMUS contract requirements. No relevant exceptions were noted. The information reviewed confirms management's description.
19. Access to the data center is restricted to authorized personnel, requiring appropriate identification and authentication.	• *Tested* data center access by attempting access using badges other than those that should be authorized. • *Inspected* data center visitor log and noted the dates, times, visitors, and the purposes of those visits. • *Discussed* data center access policies and rules with the Technical Infrastructure Manager.	No relevant exceptions were noted. The tests performed confirm management's description. No relevant exceptions were noted. The documents inspected confirm management's description. No relevant exceptions were noted. The discussions confirm management's description.

I. Information Systems General Controls		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
20. A business impact assessment has been performed that considers the impact of systems failure on the case management process.	• *Reviewed* the Business Impact Analysis prepared part of the Business Continuity (BC) / Disaster Recovery (DR) plan. • *Discussed* the feasibility of the BC/DR plan with the Technical Infrastructure Manager.	No relevant exceptions were noted. The information reviewed confirms management's description. No relevant exceptions were noted. The discussions confirm management's description. Noted that MAXIMUS is in the process of enhancing recovery strategies which will then be updated into the BC/DR plan.

I. Information Systems General Controls		
Controls Specified by MAXIMUS	**Testing Performed by the Service Auditor**	**Results of Test**
Manage Facilities		
21. Facilities are adequately secured and managed.	• *Inquired* of the Facilities Coordinator as to the security of the facilities.	No relevant exceptions were noted. The inquiries confirm management's description. Noted that the badge access is setup based upon new employee notification from HR. Both badge setup and termination is from the Help Desk notification system.
	• *Tested* the current building badge access list against the active employee list for authorized badge holders.	No relevant exceptions were noted. The tests performed confirm management's description.
	• *Tested* badge access by attempting access to inappropriate areas with various unauthorized badges and was refused access.	No relevant exceptions were noted. The tests performed confirm management's description.
	• *Observed* that to obtain building access all employees and visitors must sign-in to the building in addition to wearing badges.	No relevant exceptions were noted. The procedures observed were consistent with management's description. Noted that staff sign-in with team lead.
	• *Observed* that a building video surveillance system is operational, including a camera facing the server room door.	No relevant exceptions were noted. The procedures observed were consistent with management's description.

I. Information Systems General Controls		
Controls Specified by MAXIMUS	**Testing Performed by the Service Auditor**	**Results of Test**
22. Data center facilities are equipped with adequate environmental controls to maintain systems and data, including fire suppression, uninterrupted power service (UPS), generator, and appropriate air conditioning.	• *Inquired* of the Director of Information Services, the Technical Infrastructure Manager, and the Facilities Coordinator, regarding the environmental controls in place. • *Inspected* the following environmental controls in the computer room: ▪ 20 ton Liebert air conditioner unit ▪ CATT generator with a 5,000 fuel tank capable ▪ Fire rated door ▪ Wet pipe sprinkler system ▪ Battery backup for use during cut-over to the generator.	No relevant exceptions were noted. The inquiries confirm management's description. Noted that the generator is tested being run at full load once a year. Additionally there are weekly generator tests each Monday for fifteen (15) minutes. No relevant exceptions were noted. The documents inspected confirm management's description.

I. Information Systems General Controls		
Controls Specified by MAXIMUS	**Testing Performed by the Service Auditor**	**Results of Test**
Compliance with External Requirements		
23. Control activities are in place and followed to ensure compliance with external requirements, such as regulatory and legal rules.	• *Reviewed* various QMS documents including but not limited to: ▪ CA HFP Quality Manual ▪ Prime Contract Amendment Review ▪ Subcontractor Supplier Approval ▪ Administrative Contractor contract with the MRMIB.	No relevant exceptions were noted. The information reviewed confirms management's description.
	• *Obtained and reviewed* the California Healthy Families Performance Standards Analysis Report.	No relevant exceptions were noted. The information reviewed confirms management's description. Noted that the Performance Standards Report maps directly to the contract with the MRMIB.
	• *Reviewed* a sample of the personnel files and noted that appropriate confidentiality agreements (pertaining to HIPAA) are signed.	No relevant exceptions were noted. A statistically valid sample of sixty-four (64) employee files was selected for review noting that appropriate confidentiality agreements were signed. The tests performed confirm management's description.
	• *Inquired* of the Director of Compliance and the Enrollment/ Eligibility Manager regarding PHI security.	No relevant exceptions were noted. Discussions noted that PHI remains confidential and in compliance with HIPAA. The discussions confirm management's description.

I. Information Systems General Controls		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
24. Internal events are considered in a timely manner to support continuous compliance with legal and regulatory requirements.	• *Reviewed* various QMS documents including but not limited to: ▪ CA HFP Quality Manual ▪ Administrative Contractor contract with the MRMIB ▪ Reviewed QA audit plan and audit documentation. ▪ Reviewed the Weekly Tactical Meeting minutes.	No relevant exceptions were noted. The information reviewed confirms management's description.
	• *Obtained and reviewed* the California Healthy Families Performance Standards Analysis Report.	No relevant exceptions were noted. The information reviewed confirms management's description. Noted that the Performance Standards Report maps directly to the contract with the MRMIB.
	• *Inquired* of the Director of Compliance regarding contract requirements being monitored regularly by management.	No relevant exceptions were noted. The inquiries confirm management's description.

I. Information Systems General Controls		
Controls Specified by MAXIMUS	**Testing Performed by the Service Auditor**	**Results of Test**
Management of Quality		
25. Documentation is created and maintained for all significant processes, controls and activities.	• *Obtained and reviewed* various QMS documentation.	No relevant exceptions were noted. The information reviewed confirms management's description. Noted the use of revision dates and the document properties are updated as evidence that the documents are being maintained.
	• *Reviewed* minutes of the IPWG meeting where many of the documents are approved. Noting that the documents are formally approved in these meetings	No relevant exceptions were noted. The information reviewed confirms management's description.
26. A plan to maintain the overall quality assurance of activities, based on the Project plans, exists.	• *Reviewed* the Quality Manual and QMS Plan.	No relevant exceptions were noted. The information reviewed confirms management's description.
	• *Inquired* of the Senior Manger of Compliance as to maintaining the quality assurance of activities for Project plans.	No relevant exceptions were noted. The inquiries confirm management's description.

I. Information Systems General Controls		
Controls Specified by MAXIMUS	**Testing Performed by the Service Auditor**	**Results of Test**
27. Documentation standards are in place, have been communicated to all staff, and are supported with training.	• *Obtained and reviewed* QMS documentation.	No relevant exceptions were noted. The information reviewed confirms management's description.
	• *Inquired* of the Training Supervisor that standards do exist and are: ▪ In place ▪ Communicated to all staff ▪ Supported with training	No relevant exceptions were noted. The inquiries confirm management's description. Noted a new employee training matrix exists to ensure policies and procedures are communicated based on employee position.
	• *Inspected* various Work Instructions (WI) and noted that they provide the process documentation.	No relevant exceptions were noted. The documents inspected confirm management's description.
28. A quality plan exists for significant IT functions (e.g., large system development and deployment projects) and provides a consistent approach to address both general and project-specific quality assurance activities.	• *Reviewed* various QMS documentation including but not limited to: ▪ QA audit reports for the year ▪ CA HFP Quality Manual ▪ ISO 9000 Internal Quality Audit	No relevant exceptions were noted. The information reviewed confirms management's description.
	• *Tested* several QA audit processes during the year and reviewed the results of those audits to determine if the computations were correct.	No relevant exceptions were noted. The tests performed confirm management's description.
	• *Inquired* of the Director of Compliance about involvement in the CAR Projects.	No relevant exceptions were noted. The inquiries confirm management's description. Noted that the QA area is involved in large scale development and deployment projects.

I. Information Systems General Controls		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
29. The quality plan prescribes the type(s) of quality assurance activities (such as reviews, audits, inspections) to be performed to achieve the objectives of the quality plan.	• *Reviewed* the document CA HFP Quality Manual to determine if it prescribes the type(s) of quality assurance activities (such as reviews, audits, inspections) to be performed.	No relevant exceptions were noted. The information reviewed confirms management's description.
30. The quality assurance process includes a review of adherence to policies, procedures and standards.	• *Reviewed* various QMS documentation including but not limited to: ▪ CA HFP Quality Manual ▪ ISO 9000 Internal Quality Audit ▪ Corporate QA Best Practices Checklist	No relevant exceptions were noted. The information reviewed confirms management's description.
	• *Inquired* of the Director of Compliance as to the quality assurance process.	No relevant exceptions were noted. The inquiries confirm management's description.
	• *Reviewed* sample reports that alert managers regarding procedure or work instruction review.	No relevant exceptions were noted. The information reviewed confirms management's description.

I. Information Systems General Controls		
Controls Specified by MAXIMUS	**Testing Performed by the Service Auditor**	**Results of Test**
Manage Performance and Capacity		
31. IT management monitors the performance and capacity levels of the systems and network.	• *Inquired* of the Technical Infrastructure Manager as to the procedure in place to monitor performance and capacity of the systems and the network.	No relevant exceptions were noted. The inquiries confirm management's description.
	• *Reviewed* onscreen reporting and trends provided by Nagios for completeness.	No relevant exceptions were noted. The information reviewed confirms management's description.
32. IT management has a process in place to respond to suboptimal performance and capacity measures.	• *Inspected* a sample of Help Desk entries of such issues noting conformity with stated policy.	No relevant exceptions were noted. A statistically valid sample of sixty-eight (68) Help Desk entries was selected noting conformity with stated policies. The tests performed confirm management's description.
	• *Inspected* a completed Performance Solution Analysis document that was presented to upper management.	No relevant exceptions were noted. The document inspected confirms management's description.
	• *Inquired* of the Technical Infrastructure Manager as to the procedure noting conformity with the stated process.	No relevant exceptions were noted. The inquiries confirm management's description.

I. Information Systems General Controls		
Controls Specified by MAXIMUS	**Testing Performed by the Service Auditor**	**Results of Test**

33. Performance and capacity planning is included in system design and implementation activities.	• *Inspected* the following:
	   ■ A sample of CARs in all status levels was selected for the audit period.
	   ■ The CAR performance impact analysis documents were reviewed for all relevant CARs.
	
	• *Inquired* of the Manager of Software Engineering concerning:
	   ■ Scheduling of the implementations
	   ■ Impact analysis process
	   ■ Peer review and code performance
		No relevant exceptions were noted.
		A statistically valid sample of fifty-seven (57) problem statements associated with the sample CARs were selected for inspection. The tests performed confirm management's description.
		
		No relevant exceptions were noted. The inquiries confirm management's description.

I. Information Systems General Controls		
Controls Specified by MAXIMUS	**Testing Performed by the Service Auditor**	**Results of Test**
Monitoring		
34. Performance indicators or benchmarks, from both internal and external sources, have been defined, and data is collected and reported regarding achievement of these benchmarks.	• *Reviewed* various documentation including but not limited to: ▪ CAHFP Performance Standards Report ▪ Weekly Risk Assessment Reports ▪ Call Center Report ▪ Weekly and Monthly Administrative Vendor Reports ▪ Project Status Report • *Sampled* the CAHFP Performance Standards Report by contacting the individual departments responsible for reporting the standards and tracing to the source documents.	No relevant exceptions were noted. The information reviewed confirms management's description. No relevant exceptions were noted. A sample of the Performance Standards Report was selected for tracing to the source documents. The tests performed confirm management's description.

I. Information Systems General Controls		
Controls Specified by MAXIMUS	**Testing Performed by the Service Auditor**	**Results of Test**
35. Management has established appropriate metrics to effectively manage the day-to-day activities.	• *Reviewed* various documentation including but not limited to: ▪ CAHFP Performance Standards Report ▪ Weekly Risk Assessment Reports ▪ Call Center Report ▪ Weekly and Monthly Administrative Vendor Reports ▪ Project Status Report	No relevant exceptions were noted. The information reviewed confirms management's description.
	• *Sampled* the CAHFP Performance Standards Report by contacting the individual departments responsible for reporting the standards and tracing to the source documents.	No relevant exceptions were noted. A sample of the Performance Standards Report was selected for tracing to the source documents. The tests performed confirm management's description.
	• *Inquired* of various Project Managers as well as the Financial Operations Director regarding metrics that manage day-to-day activities.	No relevant exceptions were noted. The inquiries confirm management's description.

I. Information Systems General Controls		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test

36. Management monitors delivery of services to identify shortfalls and responds with actionable plans to improve.	• *Reviewed* various documentation including but not limited to:
	  ▪ CAHFP Performance Standards Report
	  ▪ Weekly Risk Assessment Reports
	  ▪ Call Center Report
	  ▪ Weekly and Monthly Administrative Vendor Reports
	  ▪ Project Status Report
		No relevant exceptions were noted. The information reviewed confirms management's description.

	• *Inquired* of the Director of Compliance as to the procedures and practices that are performed to monitor, identify and improve on services performed.	No relevant exceptions were noted. The inquiries confirm management's description.

I. Information Systems General Controls		
Controls Specified by MAXIMUS	**Testing Performed by the Service Auditor**	**Results of Test**
Adequacy of Internal Control		
37. Management monitors the effectiveness of internal controls in the normal course of operations through management and supervisory activities, comparisons and benchmarks.	• *Inquired* of the Deputy Project Manager as well as the Financial Operations Director and the Human Resources Director regarding the monitoring of the effectiveness of internal controls in the normal course of operations.	Obtained and reviewed the Monthly Risk Assessment reports. A sample of fourteen (14) individual summary statistics used for the monthly risk assessment was selected for tracing to the source documents. The tests performed confirm management's description.
38. Serious deviations in the operation of internal control, including major security, availability and processing integrity events, are reported to senior management.	• *Inquired* of the Director of Information Systems and discussed the procedures of informing management of deviations in the operation of internal control, including major security, availability and processing integrity events. • *Obtained* and *reviewed* the Outage Summary report (includes information from 2006 to current). • *Reviewed* various documentation including but not limited to: ▪ Mercury ITG logs ▪ CAR logs ▪ Meeting minutes discussing problem statements and CARS.	Obtained and reviewed the Monthly Risk Assessment reports. A sample of fourteen (14) individual summary statistics used for evaluating risk was selected for tracing to the source documents. The tests performed confirm management's description. No relevant exceptions were noted. The information reviewed confirms management's description. No relevant exceptions were noted. The information reviewed confirms management's description.

I. Information Systems General Controls

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
39. Internal control assessments are performed periodically, using self-assessments, to examine whether or not internal controls are operating satisfactorily.	• *Inquired* of the Director of Compliance as to the procedures for informing management of deviations in the operation of internal control, including major security, availability and processing integrity events.	No relevant exceptions were noted. The inquiries confirm management's description.
	• *Discussed* the procedures and practices in place to examine if internal controls are operating satisfactorily.	No relevant exceptions were noted. The discussions confirm management's description.
	• *Obtained* and *reviewed* the Outage Summary report at February 6, 2009 (includes historic information from 2006).	No relevant exceptions were noted. The information reviewed confirms management's description.
	• *Reviewed* various documentation that would include an indication of internal control deviations including but not limited to: ▪ Mercury ITG logs ▪ CAR logs ▪ Meeting minutes discussing problem statements and CARS ▪ Risk Assessment reports ▪ QA inspections reports ▪ Management review meeting minutes.	No relevant exceptions were noted. The information reviewed confirms management's description.

I. Information Systems General Controls		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
Internal Audit		
40. Agreed-upon Procedures (AUP) and Internal Audit engagements are performed based on approval by the audit committee.	• *Reviewed* various AUP and Internal Audit reports.	No relevant exceptions were noted. The information reviewed confirms management's description.
	• *Reviewed* the approved schedule of AUP and Internal Audits.	No relevant exceptions were noted. The information reviewed confirms management's description. Noted the September 2008 AUP was not performed.
	• *Compared* AUP reports and internal audits against approved schedule of AUP and Internal Audits.	No relevant exceptions were noted. The information reviewed confirms management's description. Noted that AUP and Internal Audit engagements were performed other than the one scheduled for September 2008 based on approval by the audit committee.

I. Information Systems General Controls		
Controls Specified by MAXIMUS	**Testing Performed by the Service Auditor**	**Results of Test**
Third-Party Services		
41. A designated individual is responsible for regular monitoring and reporting on the achievement of the third-party service level performance criteria.	• *Reviewed* the Supplier / Subcontractor Performance Standards Analysis Report for compliance with the control. • *Reviewed* the QMS document Subcontractor Supplier Approval. • *Inquired* of the Contracts Manager as to the procedures in place to monitor the third-party service level performance criteria.	No relevant exceptions were noted. The information reviewed confirms management's description. No relevant exceptions were noted. The information reviewed confirms management's description. No relevant exceptions were noted. The inquiries confirm management's description.

42. The selection of vendors for outsourced services is performed in accordance with the Project's vendor management policy.	• *Inquired* of the Contracts Manager that the Project complies with the Authority and Responsibility Policies and Procedures Manual.
	
	• *Reviewed* various documentation including but not limited to:
	   ▪ Authority and Responsibility Policies and Procedures Manual
	   ▪ Vendor contracts and compliance matrix with outsource vendors
	   ▪ Subcontractor supplier approval
		No relevant exceptions were noted. The inquiries confirm management's description. Noted that evaluation criteria is generated during solicitation planning and due diligence is used to collect a minimum of three written competitive quotations
		
		No relevant exceptions were noted. The information reviewed confirms management's description.

I. Information Systems General Controls		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
43. Before selection, management determines that potential third parties are properly qualified through an assessment of their capability to deliver the required service.	• *Inquired* of the Contracts Manager that the Project uses an RFP process to review the qualifications of vendors prior to their being contracted to perform services. • *Reviewed* Subcontractor Supplier Approval which specifies guidelines for: ▪ Maintenance of the CA HFP Sub-Contracts through amendments and clarifications. ▪ Ensuing adherence and retention of the CA HFP Prime Contract through the evaluation of Subcontractors. ▪ Negotiation and award of Subcontracts under the CA HFP Prime Contract. ▪ Record of contract negotiations, contract review, amendments, and clarifications.	No relevant exceptions were noted. The inquiries confirm management's description. Noted that potential vendors are assessed, exceptions to Subcontractor Agreement Package are appraised, and a financial impact review completed for Executive Management. No relevant exceptions were noted. The information reviewed confirms management's description.

I. Information Systems General Controls		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test

44. Third-party service contracts address the risks, security controls and procedures for information systems and networks in the contract between the parties.	• *Reviewed* the existing vendor contracts with the Contracts Manager.
	
	• *Reviewed* Subcontractor Supplier Approval which specifies guidelines for:
	  ▪ Maintenance of the CA HFP Sub-Contracts through amendments and clarifications.
	  ▪ Ensuing adherence and retention of the CA HFP Prime Contract through the evaluation of Subcontractors.
	  ▪ Negotiation and award of Subcontracts under the CA HFP Prime Contract.
	  ▪ Record of contract negotiations, contract review, amendments, and clarifications.
		No relevant exceptions were noted. The information reviewed confirms management's description.
		
		No relevant exceptions were noted. The information reviewed confirms management's description.

I. Information Systems General Controls		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
45. Procedures exist and are followed to ensure that a formal contract is defined and agreed to for all third-party services before work is initiated, including definition of internal control requirements and acceptance of the Project's policies and procedures.	• *Inquired* of the Contracts Manager to verify that the Project complies with the Authority and Responsibility Policies and Procedures Manual.	No relevant exceptions were noted. The inquiries confirm management's description. Noted that Evaluation of Subcontractor Proposal Award Phase is followed. Negotiations are conducted and Corporate Legal is consulted as appropriate before a contract is signed. The Authority Matrix is reviewed for appropriate signing authority.
	• *Reviewed* various documentation including but not limited to: ▪ Authority and Responsibility Policies and Procedures Manual ▪ Vendor Contracts and Compliance Matrix with Outsource Vendors ▪ Subcontractor Supplier Approval	No relevant exceptions were noted. The information reviewed confirms management's description.

I. Information Systems General Controls		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
46. A regular review of security, availability and processing integrity is performed for service level agreements and related contracts with third-party service providers.	• *Inquired* of the Contracts Manager as to the procedures in place to review the availability and processing integrity for service level agreements.	No relevant exceptions were noted. The inquiries confirm management's description.
	• *Reviewed* Subcontractor Supplier Approval which provides guidelines for: ▪ Maintenance of the Subcontracts by amendments and clarifications. ▪ Ensuing adherence and retention of the Prime Contract through the evaluation of Subcontractors. ▪ Negotiation and award of Subcontracts under the Prime Contract. ▪ Record of contract negotiations, contract review, amendments, and clarifications.	No relevant exceptions were noted. The information reviewed confirms management's description.
	• *Reviewed* the vendor contracts and compliance matrix with the Contracts Manager.	No relevant exceptions were noted. The information reviewed confirms management's description.

II. Computer Operations Controls		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
Control Objective 2: Controls provide reasonable assurance that any problems and/or incidents are properly responded to, recorded, resolved, or investigated for proper resolution.		
1. IT management has defined and implemented a problem correction system that ensures operational events (breakage, problems and errors) not part of the standard operation, are recorded, analyzed and resolved in a timely manner.	• *Inspected* a sample of Help Desk entries for completeness. Tracked the sample from entry to resolution and obtained proof of resolution where available.	A statistically valid sample of sixty-eight (68) Help Desk entries was selected for inspection. The tests performed confirm management's description. Inspection of Help Desk entries revealed one (1) exception with three instances where the Help Desk entries did not conform to stated policies and procedures. **MAXIMUS Response:** These three instances are associated with documentation level in Mercury ITG (IT Governance Center), which is a tool used to process Help Desk tickets. The first instance was a Help Desk entry from Systems, where the SLA was not met because the priority was not updated. The second instance was also a Help Desk entry from Systems, in which a note was not entered when the priority was updated. The third instance was a Help Desk entry assigned to the Facilities Department. The completion of a request was not documented in ITG after it was processed.

II. Computer Operations Controls		
Controls Specified by MAXIMUS	**Testing Performed by the Service Auditor**	**Results of Test**
		Systems and Facilities staff have attended a training refresher on the procedures to ensure that proper levels of documentation are entered into ITG.
		Problem Statement #55426 has been generated for staff training refresher and preventive action plans.
	• *Inquired* of the Technical Infrastructure Manager as to the problem management policies and procedures noting conformity with stated policy.	No relevant exceptions were noted. The inquiries confirm management's description.
2. The problem management system provides adequate audit trail facilities, which allows tracing from incident to underlying cause.	• *Inspected* a sample of Help Desk entries for completeness. Traced from entry to resolution and obtained proof of resolution when available.	No relevant exceptions were noted. A statistically valid sample of sixty-eight (68) Help Desk entries was selected for tracing for completeness. The tests performed confirm management's description.
	• *Inquired* of the Technical Infrastructure Manager as to the problem management system audit trail policies and procedures noting conformity with stated policy.	No relevant exceptions were noted. The inquiries confirm management's description.

II. Computer Operations Controls		
Controls Specified by MAXIMUS	**Testing Performed by the Service Auditor**	**Results of Test**
3. A security incident response process exists to support timely response and investigation of unauthorized activities.	• *Inquired* of the Technical Infrastructure Manager as to the security incident response policies and procedures noting conformity with stated policy.	No relevant exceptions were noted. The inquiries confirm management's description.
	• *Reviewed* the Help Desk processes and procedures related to security incident response.	No relevant exceptions were noted. The information reviewed confirms management's description.
	• *Inquired* of the Technical Infrastructure Manager regarding the involvement of the Information Security Administrator in responding to a security incident.	No relevant exceptions were noted. The inquiries confirm management's description.
4. A contingency plan exists for alternative processing in the event of loss or interruption of the IT function.	• *Reviewed* the Contingency Plan BC/DR plan.	No relevant exceptions were noted. The information reviewed confirms management's description.
	• *Discussed* the feasibility of the BC/DR plan with the Technical Infrastructure Manager.	No relevant exceptions were noted. The inquiries confirm management's description. Noted that MAXIMUS is in the process of enhancing recovery strategies which will then be updated into the BC/DR Plan.

II. Computer Operations Controls		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
Control Objective 3: Controls provide reasonable assurance that data recorded, processed and reported remains complete, accurate and valid throughout the update and storage process.		

1. Policies and procedures exist for the handling, distribution and retention of data and reporting output.	• *Reviewed* the following:
	  ▪ MAXIMUS Information Security Policy
	  ▪ Security and Confidentiality Policy
	  ▪ Backup and off-site storage procedures.
		No relevant exceptions were noted. The information reviewed confirms management's description.

	• *Inquired* of the Technical Infrastructure Manager:
	  ▪ All files sent to vendors are transported by secure carrier
	  ▪ Backup and storage files are transported by secure courier
	  ▪ All files distributed outside the Project are either encrypted or transported by a secure courier
		No relevant exceptions were noted. The inquiries confirm management's description. Noted that backup media tapes are encrypted as data is written to the media.

	• *Inspected* the following:
	  ▪ Public certificates for all vendors where data is shared electronically
	  ▪ A nightly file transfer log utilizing the public certificates
		No relevant exceptions were noted. The documents inspected confirm management's description.

II. Computer Operations Controls		
Controls Specified by MAXIMUS	**Testing Performed by the Service Auditor**	**Results of Test**

2. Management protects sensitive information, logically and physically, in storage and during transmission against unauthorized access or modification.	• *Inquired* of the Technical Infrastructure Manager:
	  ▪ All files sent to vendors are transported by secure carrier
	  ▪ Backup and storage files are transported by secure courier
	  ▪ All files distributed outside the Project are either encrypted or transported by a secure courier
	  ▪ Virus protection is active on all desktops
	  ▪ User areas of the network are segregated by VLANs and firewalls
		No relevant exceptions were noted. The inquiries confirm management's description. Noted that backup media tapes are encrypted as data is written to the media.

	• *Inspected* the following:
	  ▪ Public certificates for all vendors where data is shared electronically
	  ▪ A nightly file transfer log utilizing the public certificates.
		No relevant exceptions were noted. The documents inspected confirm management's description.

II. Computer Operations Controls		
Controls Specified by MAXIMUS	**Testing Performed by the Service Auditor**	**Results of Test**
3. Retention periods and storage terms are defined for documents, data, programs, reports, and messages (incoming and outgoing), as well as the data (keys, certificates) used for their encryption and authentication.	• *Reviewed* the actual retention periods with the Mail Operations Manager to assure that they meet the requirements of the contract with the MRMIB. • *Inquired* of the Technical Infrastructure Manager the retention periods for electronic information. • *Observed* the hardcopy file room area and procedures noting evidence that policies and procedures exist for the handling, distribution and retention of data and reporting output.	No relevant exceptions were noted. The information reviewed confirms management's description. No relevant exceptions were noted. The inquiries confirm management's description. No relevant exceptions were noted. The procedures observed were consistent with management's description.
4. Management has implemented a strategy for cyclical backup of data and programs.	• *Reviewed* PP-17-18 – CAHFP Data Backup Procedures. • *Discussed* cyclical backup schedule with the Technical Infrastructure Manager.	No relevant exceptions were noted. The information reviewed confirms management's description. No relevant exceptions were noted. The discussions confirm management's description.

II. Computer Operations Controls		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
5. Procedures exist and are followed to periodically test the effectiveness of the restoration process and the quality of backup media.	• *Reviewed* PP-17-18 – CAHFP Data Backup Procedures. • *Discussed* the test procedures with the Technical Infrastructure Manager. • *Discussed* with the Technical Infrastructure Manager the procedures for a tape inventory audit of the off-site vendor by IS personnel on a quarterly basis.	No relevant exceptions were noted. The information reviewed confirms management's description. No relevant exceptions were noted. The discussions confirm management's description. No relevant exceptions were noted. The discussions confirm management's description.

II. Computer Operations Controls		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test

6. Changes to data structures are authorized, made in accordance with design specifications and implemented in a timely manner.	• *Reviewed* the following:
	  ▪ PP-12-01 – Corrective and Preventive Action
	  ▪ PP-17-10 – System Code Migration Procedure
	  ▪ PP-17-23 – Change Action Request (CAR)
		No relevant exceptions were noted. The information reviewed confirms management's description.

	• *Inquired* of the Manager of Software Engineering regarding the:
	  ▪ Promotion process for authorized changes to data structures and results
	  ▪ DBA role in promotions
	  ▪ Testing and validating data and reports
		No relevant exceptions were noted. The inquiries confirm management's description.

	• *Inspected* a sample of CARs to validate testing, approval and promotion of authorized changes.	No relevant exceptions were noted. A statistically valid sample of fifty-seven (57) CARs was selected to validate authorized changes. The tests performed confirm management's description.

II. Computer Operations Controls		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
Control Objective 4: Controls provide reasonable assurance that authorized programs are executed as planned and deviations from scheduled processing are identified and investigated, including controls over job scheduling, processing, error monitoring, and system availability.		

1. Management has established and documented standard procedures for IT operations, including scheduling, managing, monitoring, and responding to security, availability, and processing integrity events.	• *Reviewed* the Ticket Handling documents and documentation for completeness noting the following procedures are in place for scheduling, managing, monitoring, and responding to integrity events:
	  ▪ PP-19-25 ITS Help Desk Process
	  ▪ PP-19-27 HeA Help Desk Process Flow
	  ▪ PP-17-01 Systems Ticket Handling and Documenting
	  • PP-17-23 Infrastructure Change Control Process
	
	• *Inquired* of the Technical Infrastructure Manager regarding policies and procedures that address documentation standards for IT operations.
		No relevant exceptions were noted. The information reviewed confirms management's description.
		
		No relevant exceptions were noted. The inquiries confirm management's description.

II. Computer Operations Controls		
Controls Specified by MAXIMUS	**Testing Performed by the Service Auditor**	**Results of Test**
2. System event data is sufficiently retained to provide chronological information and logs to enable the review, examination and reconstruction of system and data processing.	• *Inquired* of the Technical Infrastructure Manager as to this process. • *Inspected* logs of a sample of servers from the period under review.	No relevant exceptions were noted. The inquiries confirm management's description. No relevant exceptions were noted. The inquiries confirm management's description. Noted that logs appear to have valid data and are retained onsite, backed to tape and retained for six (6) months.
3. System event data is designed to provide reasonable assurance as to the completeness and timeliness of system and data processing.	• *Inquired* of the Technical Infrastructure Manager as to the process in place to obtain assurance as to the completeness and timeliness of system and data processing. • *Observed* notifications of processing results for important processing.	No relevant exceptions were noted. The inquiries confirm management's description. No relevant exceptions were noted. The information reviewed confirms management's description. Noted that system event logs provide information on the start/end times and the successful completion of system processes and data processing. Email notifications are sent out automatically to key personnel notifying them of results of the processing.

II. Computer Operations Controls		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
4. Policies and procedures are followed concerning security, availability and processing integrity for packaged software products that are purchased for end-user computing.	• *Inspected* the Client Image Testing Checklist for completeness noting conformity with stated policy • *Observed* that installation files are kept in a secure directory and physical install disks are kept in a locked box in a locked room. • *Inquired* of the Manager of Software Engineering as to the procedures for testing end user software products to verify compatibility with existing systems.	No relevant exceptions were noted. The documents inspected confirm management's description. No relevant exceptions were noted. The procedures observed were consistent with management's description. No relevant exceptions were noted. The inquiries confirm management's description. Noted that end-user software products are tested by a certification process to ensure their availability and processing integrity with existing systems.
5. User-developed systems, such as spreadsheets and other end-user programs, are secured from unauthorized use.	• *Reviewed* CP-02 - Security and Confidentiality Policy. • *Discussed* security of user developed systems with the Technical Infrastructure Manager.	No relevant exceptions were noted. The information reviewed confirms management's description. No relevant exceptions were noted. The discussions confirm management's description. Noted end-user developed systems are stored in secured and controlled directories with access strictly limited.

II. Computer Operations Controls		
Controls Specified by MAXIMUS	**Testing Performed by the Service Auditor**	**Results of Test**
6. Access to user-developed systems is restricted to a limited number of users.	• *Reviewed* CP-02 - Security and Confidentiality Policy. • *Discussed* security of user developed systems with the Technical Infrastructure Manager.	No relevant exceptions were noted. The information reviewed confirms management's description. No relevant exceptions were noted. The discussions confirm management's description. Noted that user-developed systems are stored in "group" directories with access limited to users who need access to these systems. In some cases only a single user requires access; in these cases the systems are stored in "home" directory locations with user access only.

II. Computer Operations Controls		
Controls Specified by MAXIMUS	**Testing Performed by the Service Auditor**	**Results of Test**
Security and Access Controls		
Control Objective 5: Controls provide reasonable assurance that Project IT operating systems and subsystems are appropriately secured to prevent unauthorized use, disclosure, modification, damage, or loss of data.		

1. An information security policy and framework exists and has been approved by an appropriate level of executive management.	• *Reviewed* the following:
	  ▪ CP-02 Security and Confidentiality Policy. Reviewed the Revision History section noting that it is maintained on a regular basis.
	  ▪ The IPWG Minutes for December 18, 2008 and October 9, 2008.
	  ▪ The MAXIMUS Information Security Policy.
		No relevant exceptions were noted. The information reviewed confirms management's description.
		Noted that the revised HeA Help Desk Process PP-17-27 and ITS Help Desk Password Tasks, WI-19-25-01, were approved.

2. Procedures exist and are followed to authenticate all users to the system to support the validity of transactions.	• *Obtained and reviewed* the Roles and Access lists for the system and Oracle Financials. • *Inquired* of the Technical Infrastructure Manager regarding user authentication controls, as well as ensuring the validity of access rights and transaction validation.	No relevant exceptions were noted. The information reviewed confirms management's description. Noted that user access is based on job function. No relevant exceptions were noted. The inquiries confirm management's description.

II. Computer Operations Controls		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
3. Procedures exist and are followed to maintain the effectiveness of authentication and access mechanisms (e.g., regular password changes).	• *Reviewed* the MAXIMUS Information Security Policy.	No relevant exceptions were noted. The information reviewed confirms management's description.
	• *Reviewed* CP-02 - Security and Confidentiality Policy.	No relevant exceptions were noted. The information reviewed confirms management's description.
	• *Discussed* the Information Security Policy with the Technical Infrastructure Manager.	No relevant exceptions were noted. The discussions confirm management's description.
	• *Tested* the active directory LDAP making use of computer assisted tools to download the LDAP and probe it for accounts that never expire.	No relevant exceptions were noted. The information reviewed confirms management's description. Noted that only special accounts with limited access capability are set never to expire.
4. Procedures exist and are followed to ensure timely action relating to requesting, establishing, issuing, suspending, and closing user accounts.	• *Inquired* of the Technical Infrastructure Manager as to these procedures noting conformity with stated policy.	No relevant exceptions were noted. The inquiries confirm management's description.
	• *Inspected* PP-17-12 – User Add/Delete defining the process of adding or deleting a user from the system.	No relevant exceptions were noted. The documents inspected confirm management's description.

II. Computer Operations Controls		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
5. A control process exists and is followed to periodically review and confirm access rights.	• *Inquired* of the Technical Infrastructure Manager regarding the periodic process of reviewing the terminations list to ensure that terminated staff no longer has system access. • *Tested* the system access lists using computer assisted audit tools to download the current list of active users, and then comparing the list against the current employee lists to determine if any terminated employees still have access.	No relevant exceptions were noted. The inquiries confirm management's description. Noted that terminations are reviewed on a weekly basis. No relevant exceptions were noted. The tests performed confirm management's description.
6. Where network connectivity is used, appropriate controls, including firewalls, intrusion detection and vulnerability assessments, exist and are used to prevent unauthorized access.	• *Inspected* the CAHFP network diagram. • *Inquired* of the Technical Infrastructure Manager regarding the: ▪ Network configuration ▪ Controls used to prevent unauthorized access ▪ Use of Nessus on new servers prior to implementation. • *Obtained* a recent external vulnerability scan.	No relevant exceptions were noted. The information reviewed confirms management's description. No relevant exceptions were noted. The inquiries confirm management's description. No relevant exceptions were noted. The information reviewed confirms management's description.

II. Computer Operations Controls		
Controls Specified by MAXIMUS	**Testing Performed by the Service Auditor**	**Results of Test**
7. IT security administration monitors and logs security activity, and identifies and reports security violations to senior management.	• *Inquired* of Corporate Network personnel regarding the outsourcing of the network security monitoring. • *Reviewed* correspondence with the outsource vendor monitoring the security activity. • *Reviewed* scan results against the perimeter performed by MAXIMUS.	No relevant exceptions were noted. The inquiries confirm management's description. No relevant exceptions were noted. The information reviewed confirms management's description. No relevant exceptions were noted. The information reviewed confirms management's description.
8. Controls relating to appropriate segregation of duties over requesting and granting access to systems and data exist and are followed.	• *Discussed* with the Technical Infrastructure Manager and noted that HR requests user access accounts via the Help Desk process. IS personnel setup the accounts requested by HR.	No relevant exceptions were noted. The discussions confirm management's description.

II. Computer Operations Controls		
Controls Specified by MAXIMUS	**Testing Performed by the Service Auditor**	**Results of Test**
9. Access to facilities is restricted to authorized personnel and requires appropriate identification and authentication.	• *Discussed* the facility access and related policies with the Facilities Coordinator.	No relevant exceptions were noted. The discussions confirm management's description.
	• *Observed* accessing the facilities at the entry point to the building. The building has a locked entry point controlled by the Receptionist. All visitors must present an ID and are escorted throughout the facilities.	No relevant exceptions were noted. The procedures observed were consistent with management's description.

	• *Reviewed* the following documents:
	  ▪ CP-02 Security and Confidentiality Policy
	  ▪ PP-17-02 Data Center Policies and Procedures
	  ▪ Facilities Access Log
		No relevant exceptions were noted. The information reviewed confirms management's description.

II. Computer Operations Controls		
Controls Specified by MAXIMUS	**Testing Performed by the Service Auditor**	**Results of Test**
Control Objective 6: Controls provide reasonable assurance that all IT components, as they relate to security, processing and availability, are well protected, would prevent any unauthorized changes, and assist in the verification and recording of the current configuration.		
1. Only authorized software is permitted for use by employees using IT assets.	• *Reviewed* the MAXIMUS Information Security Policy.	No relevant exceptions were noted. The information reviewed confirms management's description. Noted that users are unable to install software on their local workstations, ensuring compliance with this control.
	• *Discussed* with the Technical Infrastructure Manager of the Group policy in place that prohibits personnel from installing applications on their machines.	No relevant exceptions were noted. The inquiries confirm management's description. Noted that software audits are conducted using OCS (Office Communications Server) to ensure only authorized software is installed.
2. Application software and data storage systems are properly configured to provide access based on the individual's demonstrated need to view, add, change, or delete data.	• *Tested* the current application user IDs by comparing against the current employee lists to determine if any terminated employees still have access.	No relevant exceptions were noted. The tests performed confirm management's description.
	• *Discussed* data storage and system access with the Technical Infrastructure Manager.	No relevant exceptions were noted. The inquiries confirm management's description.
	• *Reviewed* the list of user access roles and confirmed the access roles with appropriate management personnel.	No relevant exceptions were noted. The information reviewed confirms management's description.

II. Computer Operations Controls		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
3. IT management has established procedures across the project to protect information systems and technology from computer viruses.	• *Inquired* of the Technical Infrastructure Manager the information systems virus protection policies. ▪ Virus protection exists at several layers of the network ▪ Virus protection exists at the desktop ▪ Virus protection exists for email	No relevant exceptions were noted. The inquiries confirm management's description.
	• *Observed* workstation compliance with the procedures that are established to protect the Organization from computer viruses.	No relevant exceptions were noted. The procedures observed were consistent with management's description.
4. Periodic testing and assessment is performed to confirm that software and the network infrastructure is appropriately configured.	• *Inquired* of the Technical Infrastructure Manager as to the procedures in place to confirm that software and the network infrastructure are appropriately configured. Including the following: ▪ Weekly review process ▪ Monitoring using Nagios	No relevant exceptions were noted. The inquiries confirm management's description. Noted that periodically, a protocol analyzer is utilized to evaluate network performance.
	• *Inspected* onscreen reporting and trends provided by Nagios noting conformity with stated policy.	No relevant exceptions were noted. The documents inspected confirm management's description.

II. Computer Operations Controls		
Controls Specified by MAXIMUS	**Testing Performed by the Service Auditor**	**Results of Test**
Acquisition, Development and Change Controls		
Control Objective 7: Controls provide reasonable assurance that technology infrastructure is acquired so that it provides the appropriate platforms to support case management operating applications.		
1. Documented procedures exist and are followed to ensure that infrastructure systems, including network devices and software, are acquired based on the requirements of the case management applications they are intended to support.	• *Reviewed* PP-17-23, which replaced WI-17-14-01, Infrastructure Change Control Procedures. • *Discussed* the process with the Technical Infrastructure Manager. This is also included as part of the problem statement process.	No relevant exceptions were noted. The information reviewed confirms management's description. No relevant exceptions were noted. The discussions confirm management's description.
Control Objective 8: Controls provide reasonable assurance that application software is acquired or developed to effectively support case management operating requirements.		
1. The acquisition and planning process ensures that infrastructure modifications are aligned with client or the Project's specifications.	• *Reviewed* PP-17-23, which replaced WI-17-14-01, Infrastructure Change Control Procedures • *Discussed* the process with the Technical Infrastructure Manager. This is also included as part of the problem statement process.	No relevant exceptions were noted. The information reviewed confirms management's description. No relevant exceptions were noted. The discussions confirm management's description. Noted that acquisitions require supporting business case documentation.

II. Computer Operations Controls		
Controls Specified by MAXIMUS	**Testing Performed by the Service Auditor**	**Results of Test**
2. IT management ensures that users are appropriately involved in the design of applications, selection of packaged software and the testing thereof, to ensure a reliable environment.	• *Reviewed* PP-17-23, which replaced WI-17-14-01, Infrastructure Change Control Procedures • *Discussed* the process with the Technical Infrastructure Manager. This is also included as part of the problem statement process.	No relevant exceptions were noted. The information reviewed confirms management's description. No relevant exceptions were noted. The discussions confirm management's description. Noted that internally developed software follows PP-17-23 and that COTS follows the Client Image Checklist Template.
3. IT management ensures that information systems are designed to include application controls that support complete, accurate, authorized, and valid transaction processing.	• *Reviewed* Quality Management System documentation. • *Inquired* of the Technical Infrastructure Manager as to the procedures in place to ensure that information systems are designed to include application controls to support complete, accurate, authorized, and valid transaction processing.	No relevant exceptions were noted. The information reviewed confirms management's description. No relevant exceptions were noted. The discussions confirm management's description. Noted that internally developed software follows PP-17-23 and that COTS follows the Client Image Checklist Template.

II. Computer Operations Controls		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
4. Post-implementation reviews are performed to verify controls are operating effectively.	• *Inquired* of the IS Application Development Manager and the Systems Analysis Manger. • *Inspected* the CARs in the Closed and PIR status.	No relevant exceptions were noted. The inquiries confirm management's description. No relevant exceptions were noted. A statistically valid sample of fifty-seven (57) CARs was selected for inspection. The tests performed confirm management's description. Noted the CAR remains open after promotion of the change and the system is monitored as part of the PIR. Approval for closure is given by the business owner.

II. Computer Operations Controls		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
Control Objective 9: Controls provide reasonable assurance that systems are appropriately tested and validated prior to being placed into production processes, and that associated controls operate as intended and support case management operating requirements.		
1. A testing strategy is followed for all significant changes in applications and infrastructure technology, which addresses unit-, system-, integration- and user acceptance-level testing to help ensure that deployed systems operate as intended.	• *Inspected* PP-17-23 – Change Action Request. • *Sampled* the CAR database and traced the relevant CARS back to the source documents to verify compliance to the testing process.	No relevant exceptions were noted. The documents inspected confirm management's description. No relevant exceptions were noted. A statistically valid sample of fifty-seven (57) CARs was selected for verification of compliance with testing process. The tests performed confirm management's description.

II. Computer Operations Controls

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
2. Interfaces with other systems are tested to confirm that data transmissions are complete, accurate and valid.	• *Obtained* and *reviewed* a sample of dates for cash receipts from: ▪ Aquracy ▪ Credit Card ▪ EFT ▪ Western Union • *Tested* to ensure that the batch total transferred agreed to the file total, then traced to the posting in Oracle Financials (for both HFP and AIM).	No relevant exceptions were noted. Statistically valid samples of dates for cash receipts, consisting of forty-eight (48) from Aquarcy, sixty-one (61) from Credit Card, thirteen (13) from EFT, and fifty-four (54) from Western Union, were selected for review. The tests performed confirm management's description. No relevant exceptions were noted. The tests performed confirm management's description. Noted where the batch interface program between the 3rd party software and Oracle Financials detected differences, an error was produced and the batch was reposted for the correct amount.

II. Computer Operations Controls

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test

3. The conversion of data is tested between its origin and its destination to confirm that it is complete, accurate and valid.	• *Reviewed* batch controls of import files for:
	  ▪ Aquarcy
	  ▪ Western Union
	  ▪ EFT
	  ▪ Credit Card
	
	• *Traced* footed file totals to the batch footer. Traced the total posted to the general ledger to the total in the batch footer.
		No relevant exceptions were noted. The information reviewed confirms management's description.
		
		No relevant exceptions were noted.
		Statistically valid samples of dates for cash receipts, consisting of forty-eight (48) from Aquarcy, sixty-one (61) from Credit Card, thirteen (13) from EFT, and fifty-four (54) from Western Union, were selected for review. The tests performed confirm management's description.
		Noted where the batch interface program between the 3rd party software and Oracle Financials detected differences, an error was produced and the batch was reposted for the correct amount.

II. Computer Operations Controls		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
Control Objective 10: Controls provide reasonable assurance that policies and procedures defining required acquisition and maintenance processes have been developed and are maintained, and that they define the documentation needed to support the proper use of the applications and the technological solutions put in place.		
1. Policies and procedures have been created for the development of system specifications.	• *Inspected* the following: ▪ PP-10-05 – Handling and Control of Fast Alerts and Program Alerts ▪ PP-12-01 – Corrective and Preventive Action ▪ PP-17-00 – Information Systems Department Overview ▪ PP-17-23 – Change Action Request (CAR) ▪ WI-17-10-01 – The System Code Migration Procedure ▪ The SRS documents for the relevant CARS selected from the random sample.	No relevant exceptions were noted. The documents inspected confirm management's description.

II. Computer Operations Controls		
Controls Specified by MAXIMUS	**Testing Performed by the Service Auditor**	**Results of Test**
2. System development policies and procedures are regularly reviewed, updated and approved by management.	• *Inspected* the following: ▪ PP-12-02 – ISO 9000 Internal Quality Audits ▪ PP-12-09 – Key Process Reviews ▪ PP-10-01 – Document Creation and Control	No relevant exceptions were noted. The documents inspected confirm management's description.
	• *Inquired* of the Director of Compliance and the Training Supervisor regarding the: ▪ Policy and procedure review process. ▪ Reporting and tracking of the policy and procedure update process.	No relevant exceptions were noted. The inquiries confirm management's description.

II. Computer Operations Controls		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
3. Project management ensures that systems and applications are developed in accordance with supported, documented policies and procedures.	• *Inspected* the following: ▪ PP-10-05 – Handling and Control of Fast Alerts and Program Alerts ▪ PP-12-01 – Corrective and Preventive Action ▪ PP-17-00 – Information Systems Department Overview ▪ PP-17-23 – Change Action Request (CAR) ▪ WI-17-10-01 – The System Code Migration Procedure	No relevant exceptions were noted. The documents inspected confirm management's description.
	• *Inspected* a sample of CARs and traced through their respective processes.	No relevant exceptions were noted. A statistically valid sample of fifty-seven (57) CARs was selected for compliance inspection. The tests performed confirm management's description.
	• *Inquired* of the Manager of Software Engineering and the Director of Compliance regarding policies and procedures that govern systems and application development efforts.	No relevant exceptions were noted. The inquiries confirm management's description.

II. Computer Operations Controls		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
Control Objective 11: Controls provide reasonable assurance that system changes of operational significance are appropriately tested and authorized before movement into production.		
1. Requests for program changes, system changes and maintenance (including changes to system software) are standardized, documented, and subject to formal change management procedures.	• *Inspected* the following: ▪ PP-17-23 – Change Action Request (CAR) ▪ PP-12-09 – Key Process Reviews ▪ PP-12-01 – Corrective and Preventive Action ▪ WI-17-10-01 – The System Code Migration Procedure	No relevant exceptions were noted. The documents inspected confirm management's description.
	• *Inquired* of the Manager of Software Engineering and the Director of Compliance.	No relevant exceptions were noted. The inquiries confirm management's description.
	• *Inspected* a sample of problem statements.	No relevant exceptions were noted. A statistically valid sample of fifty-seven (57) problem statements was selected for compliance inspection. The tests performed confirm management's description.

II. Computer Operations Controls		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test

2. Emergency change requests are documented and subject to formal change management procedures.	• *Inspected* the following:
	  ▪ PP-10-05 – Handling and Control of Fast Alerts and Program Alerts
	  ▪ PP-17-23 – Change Action Request (CAR)
	
	• *Inquired* of the Manager of Software Engineering.
		No relevant exceptions were noted. The documents inspected confirm management's description.
		
		No relevant exceptions were noted. The inquiries confirm management's description.

3. Controls are in place to restrict migration of programs to production only by authorized individuals.	• *Inspected* the following:
	  ▪ PP-17-10 – The System Code Migration Procedure
	  ▪ WI-17-10-01 – The System Code Migration Procedure
	
	• *Inquired* of the Manager of Software Engineering regarding the process of migration to production.
		No relevant exceptions were noted. The documents inspected confirm management's description.
		
		No relevant exceptions were noted. The inquiries confirm management's description. Noted that access is rotated among senior developers on a monthly basis. A separate sign-on is used and the password is changed each rotation.

II. Computer Operations Controls		
Controls Specified by MAXIMUS	**Testing Performed by the Service Auditor**	**Results of Test**
4. IT Management ensures that setup and implementation of system software do not jeopardize the security of the data and programs stored on the system.	• *Inquired* of the Manager of Software Engineering. • *Inspected* relevant CARs from a sample. CARs were traced through the recovery procedure.	No relevant exceptions were noted. The inquiries confirm management's description. No relevant exceptions were noted. A statistically valid sample of fifty-seven (57) CARs was selected for compliance inspection. The tests performed confirm management's description.

III. HFP and AIM – Application Controls – Input, Processing and Output		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
Input Controls		
Control Objective 12: Input controls provide reasonable assurance that: • Originating HFP and AIM source data enters into the system through trained and authorized persons, and that data preparation procedures are established and followed to minimize errors and omissions, and to allow the input of only valid data into the system. • Authorized source documentation and data is complete and accurate, properly accounted for, and transmitted in a timely manner. • Error handling procedures detect errors and irregularities and report them for corrective action. • Source documents are retained and available for reconstruction and legal compliance.		

1. Written procedures and work instructions establish business-related functional process flows and define job tasks. Personnel receive procedure training.	• *Inspected* the following:
	   ▪ PP-03-01 – SPE Data Entry
	   ▪ PP-05-02 – Case Correction Request
	   ▪ WI-02-02-02 – Initial Receipt and Determination
	   ▪ WI-02-02-01 – Missing Info for HFP Apps
	
	• *Inquired* of the Training Supervisor regarding training procedures.
		No relevant exceptions were noted. The documents inspected confirm management's description.
		
		No relevant exceptions were noted. The inquiries confirm management's description.

III. HFP and AIM – Application Controls – Input, Processing and Output		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
2. Personnel are organized by function and provided access to information systems in terms of job needs. Critical input functions are separate from critical processing functions. Approval and review processes are constructed to match authority levels, provide cross-functional oversight, and ensure contractual performance.	• *Inspected* the following: ▪ PP-03-01 – SPE Data Entry ▪ PP-05-02 – Case Correction Request ▪ WI-02-02-02 – Initial Receipt and Determination ▪ WI-02-02-01 – Missing Info for HFP Apps	No relevant exceptions were noted. The documents inspected confirm management's description.
	• *Observed* the data entry and review process for all levels according to the workflow in PP-03-01 – SPE Data Entry.	No relevant exceptions were noted. The procedures observed were consistent with management's description.
	• *Inquired* of the Manager of Enrollment/Eligibility regarding segregation of duties between individuals performing data entry and performing approval and review processes.	No relevant exceptions were noted. The inquiries confirm management's description.

III. HFP and AIM – Application Controls – Input, Processing and Output		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
3. Through a multi-tiered system design, logical and physical segregation restricts data input functions to only authorized personnel. Configuration of online work queue systems limits access to only authorized personnel. Access for the system is controlled through three levels: application privilege is granted by role, database access is controlled by DBA assignment (locked or open), and the operating system administrator requires a user profile for identification setup.	• *Obtained and reviewed* the access rights information for the system. • *Inquired* of the Technical Infrastructure Manager regarding the access for the system is controlled through three levels: application privilege is granted by role, database access is controlled by DBA assignment (locked or open), and the operating system administrator requires a user profile for identification setup.	No relevant exceptions were noted. The information reviewed confirms management's description. Noted that the design of the system provides different access rights based on the users position. No relevant exceptions were noted. The inquiries confirm management's description.

III. HFP and AIM – Application Controls – Input, Processing and Output		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test

4. Automation is used for preparing documentation and entering data to minimize errors entering or occurring in the system.	• *Inspected* the following:
	  ▪ PP-01-06 - Mail Operations Incoming Nonconforming Product
	  ▪ PP-03-01 – SPE Data Entry
	  ▪ PP-05-02 – Case Correction Request
	  ▪ WI-01-03-03 - Document Imaging
	  ▪ WI-01-03-04 - Mail Operations Request for Information (RFI) Process
	  ▪ WI-02-02-02 – Initial Receipt and Determination
		No relevant exceptions were noted. The documents inspected confirm management's description.

	• *Observed* with the Manager of Enrollment/Eligibility the mailroom processing of documentation.	No relevant exceptions were noted. The procedures observed were consistent with management's description.

III. HFP and AIM – Application Controls – Input, Processing and Output		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
5. Configuration of online work queue systems route prioritized data and jobs to appropriate personnel.	• *Inspected* with the Manager of Enrollment/Eligibility the following: ▪ PP-03-01 – SPE Data Entry ▪ PP-05-02 – Case Correction Request ▪ WI-02-02-02 – Initial Receipt and Determination ▪ WI-02-02-01 – Missing Info for HFP Apps	No relevant exceptions were noted. The inquiries confirm management's description.
	• *Tested* a sample selected from applications documented on the Data Entry Specialists activity log to trace to the appropriate work queue.	No relevant exceptions were noted. The tests performed confirm management's description.
	• *Observed* the workflow process for the relevant applications as defined in PP-03-01 – SPE Data Entry.	No relevant exceptions were noted. The procedures observed were consistent with management's description.
6. Unique system-generated document control numbers are created through interactive user input with the system.	• *Inspected* WI-01-03-03 – Document Imaging	No relevant exceptions were noted. The documents inspected confirm management's description.
	• *Observed* with the Manager of Enrollment/Eligibility the document imaging process and the auto assignment of DCN numbers to the documents scanned.	No relevant exceptions were noted. The procedures observed were consistent with management's description.

III. HFP and AIM – Application Controls – Input, Processing and Output		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
7. Data flow is monitored through manual and application processes.	• *Inspected* the following: ▪ PP-01-03 – Mail Operations – Incoming ▪ PP-01-06 – Mail Operations Incoming Nonconforming Product ▪ WI-01-03-02 – Prepare Documents for Scanning ▪ WI-01-03-03 – Document Imaging ▪ WI-01-03-04 – Mail Operations Request for Information (RFI) Process	No relevant exceptions were noted. The documents inspected confirm management's description.
	• *Observed* with the Manager of Enrollment/Eligibility the flow and reconciliation of reports and logs.	No relevant exceptions were noted. The procedures observed were consistent with management's description.
	• *Inquired* of the Manager of Enrollment/Eligibility regarding the process workflow system, work queues and monitoring.	No relevant exceptions were noted. The inquiries confirm management's description.
8. The system uses GUI predefined forms, embedded interactive feedback, validation, and edit checks.	• *Observed* several systems screens utilized by the Data Entry, Eligibility, and Case Corrections departments.	No relevant exceptions were noted. The procedures observed were consistent with management's description.

III. HFP and AIM – Application Controls – Input, Processing and Output		
Controls Specified by MAXIMUS	**Testing Performed by the Service Auditor**	**Results of Test**

9. Data enters the system close to the originating source.	• *Inspected* the following:
	  ▪ PP-03-01 – SPE Data Entry
	  ▪ PP-05-02 – Case Correction Request
	  ▪ WI-02-02-02 – Initial Receipt and Determination
	  ▪ WI-02-02-01 – Missing Info for HFP Apps
		No relevant exceptions were noted. The documents inspected confirm management's description.

	• *Inquired* of the Manager of Enrollment/Eligibility regarding the data entry workflow documented in PP-03-01 – SPE Data Entry.	No relevant exceptions were noted. The inquiries confirm management's description.
	• *Observed* the SPE entry process with several data entry operators.	No relevant exceptions were noted. The procedures observed were consistent with management's description.

III. HFP and AIM – Application Controls – Input, Processing and Output		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test

10. Originating data and source documentation are stored for retention needs. The Folsom facility's second floor serves as a storage area for hard documents, stored by DCN, and electronic data is stored at Iron Mountain.	• *Reviewed* the retention and storage provisions in the contract with the State of California.
	  ▪ Noted the contract requires a twelve (12) month period of original contracts to be retained.
	  ▪ Letter of Instruction 07-10 Records Retention, changed the retention period from twelve (12) months to three (3) months.
		No relevant exceptions were noted. The information reviewed confirms management's description.

	• *Inquired* of the Manager of Enrollment/Eligibility regarding the storage and retention policy.	No relevant exceptions were noted. The inquiries confirm management's description.
	• *Observed* the storage facility and filing process.	No relevant exceptions were noted. The procedures observed were consistent with management's description.

III. HFP and AIM – Application Controls – Input, Processing and Output

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
Processing Controls		

Control Objective 13: Processing controls provide reasonable assurance that:

- Data is posted to the correct files, completely and accurately.
- Unauthorized changes to data are prevented.
- Database files remain complete and accurate until changes occur as a result of authorized processing.
- Procedures assure that balancing of data is made with relevant control totals. Transaction processing can be traced effectively to reconcile disrupted data.
- Continued integrity of stored data.
- Procedures establish development standards, as appropriate, for electronic transaction integrity and authenticity (atomicity, consistency, isolation, and durability).

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test

1. Written procedures and work instructions establish business-related functional process flows and define job tasks. Personnel receive procedure training.	• *Inspected* the following:
	  ▪ PP-03-01 – SPE Data Entry
	  ▪ PP-05-02 – Case Correction Request
	  ▪ WI-02-02-02 – Initial Receipt and Determination
	  ▪ WI-02-02-01 – Missing Info for HFP Apps
	
	• *Observed* the SPE entry process with several data entry operators.
		No relevant exceptions were noted. The documents inspected confirm management's description.
		
		No relevant exceptions were noted. The procedures observed were consistent with management's description.

III. HFP and AIM – Application Controls – Input, Processing and Output		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
2. Personnel are organized by function and provided access to information systems in terms of job needs. Critical input functions are separate from critical processing functions. Approval and review processes are constructed to match authority levels, provide cross-functional oversight, and ensure contractual performance.	• *Inspected* the following: ▪ PP-03-01 – SPE Data Entry ▪ PP-05-02 – Case Correction Request ▪ WI-02-02-02 – Initial Receipt and Determination ▪ WI-02-02-01 – Missing Info for HFP Apps ▪ DE CWD QC Spreadsheet ▪ Data Entry QA Worksheet	No relevant exceptions were noted. The documents inspected confirm management's description.
	• *Observed* the entire application entry process. Traced a sample through the process.	No relevant exceptions were noted. The procedures observed were consistent with management's description.

III. HFP and AIM – Application Controls – Input, Processing and Output		
Controls Specified by MAXIMUS	**Testing Performed by the Service Auditor**	**Results of Test**

3. Functional Quality Control (QC) Processes are in place and documented. Internal QC is performed by each unit. External QC is performed by the Quality Assurance department.	• *Inspected* the following:
	  ▪ PP-03-01 – SPE Data Entry
	  ▪ PP-05-02 – Case Correction Request
	  ▪ WI-02-02-02 – Initial Receipt and Determination
	  ▪ WI-02-02-01 – Missing Info for HFP Apps
	  ▪ DE CWD QC Spreadsheet
	  ▪ Data Entry QA Worksheet
	  ▪ Applications Data Entry Specialists activity log
		No relevant exceptions were noted. The documents inspected confirm management's description.

	• *Inquired* of the Data Entry Supervisor regarding the process defined in PP-03-01 – SPE Data Entry.	No relevant exceptions were noted. The inquiries confirm management's description.
	• *Tested* a sample off SPE entries by tracing them through the data entry process to the final eligibility determination.	No relevant exceptions were noted. The tests performed confirm management's description.

III. HFP and AIM – Application Controls – Input, Processing and Output		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test

4. Processing Reviews 100% of denials, CWD applications and new applications.	• *Inspected* the following:
	  ▪ PP-03-01 – SPE Data Entry
	  ▪ PP-05-02 – Case Correction Request
	  ▪ PP-12-14 – Quality Assurance Plan
	  ▪ WI-02-02-02 – Initial Receipt and Determination
	  ▪ WI-02-02-01 – Missing Info for HFP Applications
	  ▪ WI-05-01-03 – Program Reviews
	  ▪ WI-03-01-05 – CWD Referrals
	  ▪ WI-03-01-06 – Income Documentation
	  ▪ DE CWD QC Spreadsheet
	  ▪ Data Entry QA Worksheet
		No relevant exceptions were noted. The documents inspected confirm management's description.

	• *Inquired* of the Manager of Enrollment/Eligibility regarding the process defined in PP-03-01 – SPE Data Entry.	No relevant exceptions were noted. The inquiries confirm management's description.
	• *Tested* a sample of the SPE entries for notation of approval and appropriate disposition.	No relevant exceptions were noted. The tests performed confirm management's description.

III. HFP and AIM – Application Controls – Input, Processing and Output		
Controls Specified by MAXIMUS	**Testing Performed by the Service Auditor**	**Results of Test**

5. The System software Design provides field defaults, field locking and field choices which provide database normalization and control data integrity. This is achieved through the system:
• Form design
• Internal calculations
• Triggers
• FMN assignment
• Case ID assignment
• Address update
• Internal calculations
• Case ID assignment
• Verification
	• *Inspected* the following:
	  ▪ PP-03-01 – SPE Data Entry
	  ▪ PP-05-02 – Case Correction Request
	  ▪ PP-12-14 – Quality Assurance Plan
	  ▪ WI-02-02-02 – Initial Receipt and Determination
	  ▪ WI-02-02-01 – Missing Info for HFP Applications
	  ▪ WI-05-01-03 – Program Reviews
	  ▪ WI-03-01-05 – CWD Referrals
	  ▪ WI-03-01-06 – Income Documentation
	  ▪ CAR documentation
	
	• *Observed* Application Entry, Eligibility, and Case Corrections process.
		No relevant exceptions were noted. The documents inspected confirm management's description.
		
		No relevant exceptions were noted. The procedures observed were consistent with management's description.

III. HFP and AIM – Application Controls – Input, Processing and Output		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
6. Batch control and notification is used for the nightly (daily) batch update and posting of transaction records.	• *Inquired* of the Technical Infrastructure Manager.	No relevant exceptions were noted. The inquiries confirm management's description. Noted that nightly batch processes send notifications of failures, issues and successes to responsible individuals based on the batch process involved.
	• *Tested* the batch updates for deposits.	No relevant exceptions were noted. The tests performed confirm management's description. Noted where the batch interface program between the 3rd party software and Oracle Financials detected a difference, an error was produced and the batch was reposted for the correct amount.

III. HFP and AIM – Application Controls – Input, Processing and Output		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
7. Controls exist via special system user interfaces to perform case corrections in special cases. Specially assigned trained users possess special roles with higher privilege (super user) for accessing cases using separate data entry forms available to correct the cases. These users are separate from data entry or eligibility staff. All accesses to cases are noted automatically and recorded in a table.	• *Inspected* the following: 　▪ PP-17-23 – Change Action Request CAR 　▪ PP-12-17 – EOM Disenrollment Quality Analysis Plan 　▪ PP-05-02 – Case Correction Request 　▪ WI-05-02-04 – Reinstate with Capped Enrollment 　▪ WI-05-02-01 – Generating a Financial Request 　▪ WI-05-02-02 – Add A Person- No Effective Date 　▪ WI-05-02-03 – AER only give one month due to CE Noted evidence that there are independent controls around Case Corrections and Clean Ups.	No relevant exceptions were noted. The documents inspected confirm management's description.
	• *Tested* the case corrections file for the audit period.	No relevant exceptions were noted. The tests performed confirm management's description.
	• *Inquired* of appropriate personnel regarding Case Corrections and Clean Ups.	No relevant exceptions were noted. The inquiries confirm management's description.

III. HFP and AIM – Application Controls – Input, Processing and Output		
Controls Specified by MAXIMUS	**Testing Performed by the Service Auditor**	**Results of Test**
8. A dedicated Research and Appeals unit is responsible for customer interface regarding all disputes.	• *Inspected* the following: 　▪ PP-05-01 – HFP Appeals 　▪ WI-05-01-01 – Appeals Process 　▪ WI-05-01-04 – Billing Disputes 　▪ WI-05-01-05 – Case Chronologies	No relevant exceptions were noted. The documents inspected confirm management's description.
	• *Inquired* of the Manager of Enrollment/Eligibility regarding all disputes.	No relevant exceptions were noted. The inquiries confirm management's description.
	• *Tested* a sample of the appeals letter process for two months.	No relevant exceptions were noted. The tests performed confirm management's description.

III. HFP and AIM – Application Controls – Input, Processing and Output		
Controls Specified by MAXIMUS	**Testing Performed by the Service Auditor**	**Results of Test**
9. Daily backups are performed and regularly tested. Rotation methods are documented and practiced and a log is maintained. Storage of media is maintained at the Iron Mountain location.	• *Reviewed* various documentation including but not limited to: ▪ The backup procedures followed for each system. ▪ The backup logs noting any errors or warnings.	No relevant exceptions were noted. The information reviewed confirms management's description.
	• *Observed* a restore that was performed and recorded as a successful result.	No relevant exceptions were noted. The procedures observed were consistent with management's description.
	• *Obtained and reviewed* the log of items stored at the off-site storage facility.	No relevant exceptions were noted. The procedures observed were consistent with management's description.
	• *Inspected* a sample of the log of items stored at the facility with the items present at the facility.	No relevant exceptions were noted. The documents inspected confirm management's description.
	• *Inquired* of IT support personnel to determine backup procedures.	No relevant exceptions were noted. The inquiries confirm management's description.

III. HFP and AIM – Application Controls – Input, Processing and Output		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
Output Controls		
Control Objective 14: Output controls provide reasonable assurance that: • Procedures define handling and retention of output. When negotiable instruments are produced, special care is taken to prevent misuse. • Procedures define and assure appropriate distribution of IT output. • Procedures are communicated for physical and logical access to output. Confidentiality of output is defined and taken into consideration in the procedures. • Procedures assure that both provider and user review output for accuracy and that procedures control errors contained in output. • Physical access to output printers and subsequent storage areas is restricted to authorized personnel.		
1. Written procedures and work instructions establish business-related functional process flows and define job tasks. Personnel receive procedure training.	• *Reviewed* various documentation including but not limited to: ▪ SPE Data Entry ▪ Case Correction Request ▪ Initial Receipt and Determination ▪ Missing Info for HFP Applications • *Traced* a sample of employees to their respective training records for completeness.	No relevant exceptions were noted. The information reviewed confirms management's description. Noted that documented business and functional procedures exist. No relevant exceptions were noted. A statistically valid sample of twenty-eight (28) employee training records was selected for tracing to their training records for completeness. The tests performed confirm management's description.

III. HFP and AIM – Application Controls – Input, Processing and Output		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
2. Personnel are organized by function and provided access to information systems in terms of job needs. Approval and review processes are constructed to match authority levels, provide cross-functional oversight, and ensure contractual performance.	• *Reviewed* various documentation including but not limited to: ▪ SPE Data Entry ▪ Case Correction Request ▪ Initial Receipt and Determination ▪ Missing Info for HFP Applications • *Observed* in a walkthrough the data entry and review process with all levels according to the workflow in SPE Data Entry. • *Inquired* of all levels the AIM data entry and review process according to the workflow in SPE Data Entry.	No relevant exceptions were noted. The information reviewed confirms management's description. No relevant exceptions were noted. The procedures observed were consistent with management's description. No relevant exceptions were noted. The inquiries confirm management's description.
3. The System Software Design provides field defaults, field locking and field choices which control data integrity for data output. This is achieved through the system: • Triggers • Letter file generation • Filtered date-driven restrictions • 2D Barcode (KP Corp)	• *Observed* the Data entry and Eligibility processes. Noted the use of a filter for date validity field defaults, field locking and the use of 2D Barcode field choices. For eligibility noted the use of triggers for letter file generation.	No relevant exceptions were noted. The procedures observed were consistent with management's description.

III. HFP and AIM – Application Controls – Input, Processing and Output		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test

4. Batch controls exist within the system using Online 24X7 monitoring with a dedicated IT technician for batch jobs. The batch control is used for the following:
• Outbound letter files
• Mail count comparisons
• Reporting of PDF images (counts)
• Capitation calculation and preparation of 820 and 834 files.
	• *Inspected* various documentation including:
	  ▪ Capitation Processing
	  ▪ Mail Operations - - Outgoing
	  ▪ Mail Operations – Incoming
	  ▪ Printing for the Daily Letter Production
	  ▪ Inserting Daily Letter Production with Bell & Howell Inserter
	  ▪ CWD Pulls
		No relevant exceptions were noted. The documents inspected confirm management's description.

	• *Observed* procedures for mail count comparisons noting standard procedures exist and are being used.	No relevant exceptions were noted. The procedures observed were consistent with management's description.
	• *Inspected* a sample of outbound letters that were generated and compared them to the letters in the approved master file of outbound letters to ensure they were the same.	No relevant exceptions were noted. A statistically valid sample of seventy-three (73) outbound letters was selected for comparison to the approved master file letters. The tests performed confirm management's description.

III. HFP and AIM – Application Controls – Input, Processing and Output		
Controls Specified by MAXIMUS	**Testing Performed by the Service Auditor**	**Results of Test**

5. Output uses pre-designed forms and letters that have been approved by the MRMIB and are stored in QMS.	• *Reviewed* various documentation including but not limited to:
	  ▪ Mail Ops Outgoing
	  ▪ Printing for the Daily Letter Production
	  ▪ Daily Letter Production Report
		No relevant exceptions were noted. The information reviewed confirms management's description.

	• *Inspected* selected letter formats, verifying correct use of the format in outbound client correspondence.	No relevant exceptions were noted. A statistically valid sample of seventy-three (73) outbound letters was selected for comparison to the approved master file letters. The tests performed confirm management's description.

6. Error Handling – procedures exist for the handling of -
  • Returned mail
  • Letter exceptions
  • 834 and Capitation file exceptions
	• *Inspected* various documentation including:
	  ▪ 834 Exception Processing
	  ▪ Monitoring and Control of Nonconforming Product in Information Systems
	  ▪ Prepare Documents for Scanning
		No relevant exceptions were noted. The documents inspected confirm management's description.

	• *Observed* with the Manager of Enrollment/Eligibility the process for returned mail noting that returned mail is bound into groups and hand counted.	No relevant exceptions were noted. The procedures observed were consistent with management's description.

III. HFP and AIM – Application Controls – Input, Processing and Output

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
7. Activity Reporting and Monitoring includes predefined procedures for developing reports and routine report generation for monitoring output and performance.	• *Reviewed* various documentation including but not limited to: ▪ Report Development ▪ EOM Reporting Plan ▪ Daily Letter Production Report ▪ Ad Hoc Request • *Inquired* of the Director of Human Capital regarding the procedures for Activity Reporting and Monitoring.	No relevant exceptions were noted. The information reviewed confirms management's description. Noted predefined procedures for the development of reports for the monitoring of output and performance. No relevant exceptions were noted. The inquiries confirm management's description.
8. Provider Plan Capitation (Health, Vision, and Dental) - The system computes the correct amount of capitation based on the rate tables provided by the MRMIB. The amounts reported to the MRMIB are correctly allocated and summarized based on the abortion supplement (allowable funding) and the participant's legal immigration status.	• *Obtained* the 820 files for the period from July 1, 2008 to January 31, 2009. • *Obtained* the county number table. • *Obtained* the capitation rates tables used to compute the capitation amounts. • *Tested* capitation for the provider plans independently from the system using generalized audit software tools. • *Compared* the capitation amounts computed independently to those computed by the system and reported in the 820 files for the period.	No relevant exceptions were noted. No relevant exceptions were noted. No relevant exceptions were noted. No relevant exceptions were noted. The tests performed confirm management's description. No relevant exceptions were noted. The tests performed confirm management's description. Noted the AIM Lump Sum business rule. Noted the Retro-transfer business rule.

III. HFP and AIM – Application Controls – Input, Processing and Output		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
9. Prescribed capitation rates are used to correctly compute capitation.	• *Obtained* the applicable provider rate tables for the grant years being tested from the MRMIB (independent rate verification). • *Traced* the HFP provider rates obtained independently from the MRMIB to those used for computation of capitation in the system. • *Traced* the Access for Infants and Mothers (AIM) provider rates obtained independently from the MRMIB to those used for computation of capitation in the system.	No relevant exceptions were noted. The information reviewed confirms management's description. No relevant exceptions were noted. The tests performed confirm management's description. No relevant exceptions were noted. The tests performed confirm management's description.

III. HFP and AIM – Application Controls – Input, Processing and Output		
Controls Specified by MAXIMUS	**Testing Performed by the Service Auditor**	**Results of Test**
10. Capitation calculations provide for the correct allocation for allowable program funding. This includes the allocation and summarization based on the abortion supplement and the participant's legal immigration status.	• *Obtained* the "Funding Split" reports for each month for the period July 1, 2008 to January 31, 2009.	No relevant exceptions were noted.
	• *Selected* a sample of month-plan combinations from the month-plan combination population derived from the 820 files (Payment Order and Credit Advice) for the period July 1, 2008 to January 31, 2009. Parameters for the sample were: ▪ A 95% confidence level ▪ An expected error rate in the population of 5% (to assure a conservative test sample) ▪ A sampling error rate of 5%	No relevant exceptions were noted. A statistically valid sample of fifty-four (54) month-plan combinations was selected for capitation testing.
	• *Applied* the appropriate capitation rate to the totals obtained from the sample above.	No relevant exceptions were noted. The tests performed confirm management's description.
	• *Compared* the result of the capitation rate for the quantity obtained from the sample to the amount presented for the abortion rate supplement on the "Funding Split" report.	No relevant exceptions were noted. The tests performed confirm management's description.

III. HFP and AIM – Application Controls – Input, Processing and Output		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
11. Capitation and any necessary recoupments are computed and reported accurately for eligible participants in the Program. Reporting (820 files) includes accurate detailed information submitted to the MRMIB.	• *Obtained* all the 820 files (Payment Order and Credit Advice) for the period July 1, 2008 to January 31, 2009. • *Selected* a statistically valid sample from the 820 files (Payment Order and Credit Advice) for the period July 1, 2008 to January 31, 2009 (the capitation eligibility sample). The parameters for the sample were: ▪ A 95% confidence level ▪ An expected error rate in the population of 5% (to assure a conservative test sample) ▪ A sampling error rate of 5%	No relevant exceptions were noted. No relevant exceptions were noted. A statistically valid sample of seventy-three (73) participants was selected for verification of capitation eligibility.

III. HFP and AIM – Application Controls – Input, Processing and Output		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
	• *Traced* the detailed participant information to the enrollment form image retained in the system. Attributes examined included: ▪ Age on application agrees to 820 age category code ▪ County of residence agrees to 820 county code ▪ Income and family size on the application qualify client for HFP and/or AIM ▪ Plans selected per application or other documentation agree to the appropriate 820 capitation files ▪ Citizenship or immigration documentation is appropriately stored in the case file	No relevant exceptions were noted. The tests performed confirm management's description.
	• *Manually calculated* eligibility based on the information contained on the application form.	No relevant exceptions were noted. The tests performed confirm management's description.
	• *Selected* a sample of enrollments and traced them to the system to ensure the disenrollments were performed appropriately.	No relevant exceptions were noted. The tests performed confirm management's description.
12. Recoupments and replacements are performed accurately and for legitimate reasons.	• *Reviewed recoupments* in the 820 capitation file.	No relevant exceptions were noted. The information reviewed confirms management's description.

IV. Oracle Financials – HFP and AIM - Application Controls – Input, Processing and Output		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
Input Controls		
Control Objective 15: Input controls provide reasonable assurance that: • Originating HFP and AIM source data enters into Oracle Financials through trained and authorized persons, and data preparation procedures are established and followed to minimize errors and omissions, and to allow the input of only valid data into the system. • Authorized source documentation and data is complete and accurate, properly accounted, and transmitted in a timely manner. • Error handling procedures detect errors and irregularities and report them for corrective action. • Source documents are retained and available for reconstruction and legal compliance.		
1. Written procedures and work instructions establish business-related functional process flows and define job tasks. Personnel receive procedure training.	• *Reviewed* various documentation including but not limited to: ▪ Accounts Payable Reconciliation with the GL documentation ▪ Accounts Receivable Reconciliation with the GL documentation ▪ Applicable Business Rules	No relevant exceptions were noted. The information reviewed confirms management's description.
	• *Inquired* of the Project Finance Director and the Training Supervisor as to the training employees must complete with respect to their position.	No relevant exceptions were noted. The inquiries confirm management's description.
	• *Traced* a sample of employees to their respective training records for completeness.	No relevant exceptions were noted. A statistically valid sample of sixty-four (64) employee training records was selected for tracing to their training records for completeness. The tests performed confirm management's description.

IV. Oracle Financials – HFP and AIM - Application Controls – Input, Processing and Output		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
2. Personnel are organized by function and provided access to information systems in terms of job needs. Critical input functions are separate from critical processing functions. Approval and review processes are constructed to match authority levels, provide cross-functional oversight, and ensure contractual performance.	• *Reviewed* Organization charts and QMS policies for completeness and evidence of segregation of functional activities and personnel. • *Inquired* of the Project Finance Director regarding segregation of duties.	No relevant exceptions were noted. The information reviewed confirms management's description. No relevant exceptions were noted. The inquiries confirm management's description.
3. Access and Security includes the granting of access rights to the financial application based on job responsibilities and approval by the application owners via a multi-tiered system design.	• *Obtained and reviewed* the access lists for Oracle Financials. • *Inquired* of the Project Finance Director noting that authorization is based on job responsibilities.	No relevant exceptions were noted. The information reviewed confirms management's description. Noted that access rights to the financial applications are based on job responsibilities. No relevant exceptions were noted. The inquiries confirm management's description.

IV. Oracle Financials – HFP and AIM - Application Controls – Input, Processing and Output		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
4. Automated Input Systems are utilized where possible.	• *Observed* data entry functions with regards to automated Input systems with the Project Finance Director and the Supervisor for Accounts Payable/Receivable.	No relevant exceptions were noted. The procedures observed were consistent with management's description.
	• *Inquired* of the Project Finance Director and the Supervisor for Accounts Payable/Receivable noting that transactions failing edit and validation routines are posted to a suspense file. Automated input to systems is controlled.	No relevant exceptions were noted. The inquiries confirm management's description.

5. Documented procedures for the correction of errors and out-of-balance conditions and entry of overrides exist and are effectively communicated to appropriate personnel.	• *Reviewed* various documentation including but not limited to:
	  ▪ Processing Premium Adjustments.doc
	  ▪ Accounts Payable Reconciliation with GL.doc
	  ▪ Accounts Receivable Reconciliation with the GL.doc
		No relevant exceptions were noted. The information reviewed confirms management's description.

IV. Oracle Financials – HFP and AIM - Application Controls – Input, Processing and Output		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
6. Configuration of online work queue systems route prioritized data and jobs to appropriate personnel.	• *Reviewed* various documentation including but not limited to: ▪ AIM Processing documentation ▪ HFP Processing documentation ▪ DE CWD QC Process doc. ▪ Oracle Financials Systems EFT Process documentation ▪ 834 File Processing documentation	No relevant exceptions were noted. The information reviewed confirms management's description.
7. Data flow is monitored through manual and application processes.	• *Inquired* of the Project Finance Director and the Supervisor for Accounts Payable/Receivable as to the procedures in place for online data monitoring. • *Obtained and reviewed* a copy of the non-conformance log for completeness noting conformity with stated policy.	No relevant exceptions were noted. The inquiries confirm management's description. No relevant exceptions were noted. The information reviewed confirms management's description.

IV. Oracle Financials – HFP and AIM - Application Controls – Input, Processing and Output		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
8. Data enters the system close to the originating source.	• *Reviewed* process maps and noted that, with the exception of manual adjustments, all data enters Oracle Financials via batch process from outside sources: ▪ Cash Receipts – Lockbox, and EFT ▪ Invoicing – Updated from the system ▪ Refunds – Updated from the system	No relevant exceptions were noted. The information reviewed confirms management's description.
	• *Inquired* of the Systems Department that these are all close to the source origin of the transaction.	No relevant exceptions were noted. The inquiries confirm management's description.
9. Originating data and source documentation are stored for retention needs. The Folsom facility's second floor serves as a storage area for hard documents, and electronic data is stored at Iron Mountain.	• *Reviewed* storage and retention policy for completeness noting conformity with stated policy.	No relevant exceptions were noted. The information reviewed confirms management's description.
	• *Inquired* of the Systems Department, the Mail Operations Manager, and the Technical Infrastructure Manager as to the storage and retention policies and procedures.	No relevant exceptions were noted. The inquiries confirm management's description.
	• *Observed* the storage facility and viewed the filing process.	No relevant exceptions were noted. The procedures observed were consistent with management's description.

IV. Oracle Financials – HFP and AIM - Application Controls – Input, Processing and Output		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
Processing Controls		
Control Objective 16: Processing controls provide reasonable assurance that: • Data is posted to the correct files, completely and accurately. • Unauthorized changes to data are prevented. • Database files remain complete and accurate until changes occur as a result of authorized processing. • Procedures assure that balancing of data is made with relevant control totals. Transaction processing can be traced effectively to reconcile disrupted data. • Continued integrity of stored data. • Procedures establish development standards, as appropriate, for electronic transaction integrity and authenticity (atomicity, consistency, isolation, and durability).		
1. Written procedures and work instructions establish business-related functional process flows and define job tasks. Personnel receive procedure training.	• *Reviewed* Oracle Financials Systems EFT Process documentation for completeness. • *Inquired* of the Project Finance Director, the Director of Compliance, and the Training Supervisor as to the training employees must complete with respect to their position. • *Traced* a sample of employees to their respective training records for completeness.	No relevant exceptions were noted. The information reviewed confirms management's description. No relevant exceptions were noted. The inquiries confirm management's description. No relevant exceptions were noted. A statistically valid sample of twenty-eight (28) employee training records was selected for tracing training records for completeness. The tests performed confirm management's description.

IV. Oracle Financials – HFP and AIM - Application Controls – Input, Processing and Output		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
2. Personnel are organized by function and provided access to information systems in terms of job needs. Critical input functions are separate from critical processing functions. Approval and review processes are constructed to match authority levels, provide cross-functional oversight, and ensure contractual performance.	• *Inquired* of the Financial Operations Director with regards to segregation of functional activities and personnel. • *Observed* controls in place with regards to segregation of functional activities and personnel.	No relevant exceptions were noted. The inquiries confirm management's description. No relevant exceptions were noted. The procedures observed were consistent with management's description.
3. Processing reviews 100% of NSF, ACH returns and Refunds.	• *Reviewed* various QMS documentation including: ▪ Reversal of Returned items ▪ NSF Check Reversal ▪ Refund Invoice Inquiry • *Inquired* of the Supervisor for Accounts Payable/Receivable as to the procedures in place regarding Processing Reviews of NSF and ACH returns and Refunds.	No relevant exceptions were noted. The information reviewed confirms management's description. Noted the work instructions dictate the processing review functions. No relevant exceptions were noted. The inquiries confirm management's description.

IV. Oracle Financials – HFP and AIM - Application Controls – Input, Processing and Output		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
4. Standard Oracle Financials Forms (input screens) are used for interactive data entry into the financial system. Wherever possible, field verification and limits checking are performed.	• *Inquired* of the Project Controller as to the Financial Forms used with regards to controls in the software design. Noted that wherever possible, field verification and limits checking are performed. • *Observed and reviewed* with various personnel various screens noting places of field verification and limits checking.	No relevant exceptions noted. Per discussion with the Project Controller, wherever possible, field verification and limits checking are performed on inputs into Oracle Financials Forms. The inquiry confirmed management's description. No relevant exceptions were noted. The procedures observed were consistent with management's description.

IV. Oracle Financials – HFP and AIM - Application Controls – Input, Processing and Output		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
5. Batch Control exists within the Oracle Financials and all interfaces with applications and data outside Oracle Financials. Batch errors are logged and logs are reviewed.	• *Inquired* of the Project Controller as to procedures in place to obtain Batch Control. • *Obtained and reviewed* a sample of dates for cash receipts from: ▪ Aquracy ▪ Credit Card ▪ EFT ▪ Western Union • *Tested* to ensure that the batch total transferred agreed to the file total, then traced to the posting in Oracle Financials (for both HFP and AIM).	No relevant exceptions were noted. The inquiry confirmed management's description. No relevant exceptions were noted. Statistically valid samples of dates for cash receipts, consisting of forty-eight (48) from Aquarcy, sixty-one (61) from Credit Card, thirteen (13) from EFT, and fifty-four (54) from Western Union, were selected for testing. The tests performed confirm management's description. No relevant exceptions were noted. The tests performed confirm management's description. Noted that where the batch interface program between the 3rd party software and Oracle Financials detected differences, an error was produced and the batch was reposted for the correct amount.

IV. Oracle Financials – HFP and AIM - Application Controls – Input, Processing and Output		
Controls Specified by MAXIMUS	**Testing Performed by the Service Auditor**	**Results of Test**

6. Reconciliations are performed as follows:
 	
• Bank records are reconciled on a daily basis to appropriate Sub-Ledger activity.
 	
• General Ledger Cash accounts are reconciled on a monthly basis to bank records.
 	
• General Ledger Accounts Receivable and related accounts are reconciled on a monthly basis to detailed records
 	
• General Ledger Accounts Payable and related accounts are reconciled on a monthly basis to detailed records.
 	
• General Ledger control accounts are reconciled on a monthly basis to subsidiary ledger accounts on a current and regular basis.
 	
• Reconciliations are reviewed and approved on a regular basis.
	• *Reviewed* various QMS documentation including:
	  ▪ Reconciliation of the MRMIB collection
	  ▪ Reconciliation for Refunds
	  ▪ Accounts Payable Reconciliation with the General Ledger
	  ▪ Accounts Receivable Reconciliation with the General Ledger
	
	• *Inquired* of the Project Finance Director and the Supervisor for Accounts Payable/Receivable to confirm the stated policy.
	
	• *Tested* a sample of the Detailed Ledger records to the General Ledger balances.
	
	• *Tested* a sample of the accounts receivable reconciliations and accounts payable reconciliations by tracing source information (subsidiary records) to the reconciliation and agreeing the balance amounts to the general ledger control accounts.
		No relevant exceptions were noted. The information reviewed confirms management's description.
		
		No relevant exceptions were noted. The inquiries confirm management's description.
		
		No relevant exceptions were noted. The tests performed confirm management's description.
		
		No relevant exceptions were noted. The tests performed confirm management's description.

IV. Oracle Financials – HFP and AIM - Application Controls – Input, Processing and Output		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
7. Daily backups are performed and regularly tested. Rotation methods are documented and practiced and a log is maintained. Storage of media is maintained at the Iron Mountain location.	• *Reviewed* various documentation including but not limited to: ▪ The backup procedures followed for each system. ▪ The backup logs noting any errors or warnings.	No relevant exceptions were noted. The information reviewed confirms management's description.
	• *Obtained and r eviewed* the log of items stored at the off-site storage facility.	No relevant exceptions were noted. The information reviewed confirms management's description.
	• *Inspected* a sample of the log of items stored at the facility with the items present at the facility.	No relevant exceptions were noted. The documents inspected confirm management's description.
	• *Inquired* of the Technical Infrastructure Manager to determine backup procedures.	No relevant exceptions were noted. The inquiries confirm management's description.

IV. Oracle Financials – HFP and AIM - Application Controls – Input, Processing and Output

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
Output Controls		
Control Objective 17: Output controls provide reasonable assurance that: • Procedures define handling and retention of output. When negotiable instruments are produced, special care is taken to prevent misuse. • Procedures define and assure appropriate distribution of IT output. • Procedures are communicated for physical and logical access to output. Confidentiality of output is defined and taken into consideration in the procedures. • Procedures assure that both provider and user review output for accuracy and that procedures control errors contained in output. • Physical access to output printers and subsequent storage areas is restricted to authorized personnel.		
1. Written procedures and work instructions establish business-related functional process flows and define job tasks. Personnel receive procedure training.	• *Obtained and reviewed* the Oracle Financials Systems EFT Process document for completeness. • *Inquired* of the Project Finance Director, the Training Supervisor, and the Director of Compliance as to the various training employees must complete. • *Tested* a sample of staff to documentation showing that they have completed the necessary training for their respective positions.	No relevant exceptions were noted. The information reviewed confirms management's description. No relevant exceptions were noted. The inquiries confirm management's description. No relevant exceptions were noted. A statistically valid sample of twenty-eight (28) employee training records was selected for testing for completeness. The tests performed confirm management's description.

IV. Oracle Financials – HFP and AIM - Application Controls – Input, Processing and Output		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
2. Oracle Financial Software is designed with triggers and reporting.	• *Inquired* of the Project Controller as to the various triggers and reporting of the Oracle Financial Software Design.	No relevant exceptions noted. The inquiry confirmed management's description.
	• *Observed* that the Oracle Financial Software is designed with triggers and reporting.	No relevant exceptions were noted. The procedures observed were consistent with management's description.

IV. Oracle Financials – HFP and AIM - Application Controls – Input, Processing and Output		
Controls Specified by MAXIMUS	**Testing Performed by the Service Auditor**	**Results of Test**

3. Refund Output Controls include:
 	
• Refund processing produces an output file (the initial run) used by the State of California for approval prior to the final disbursement of refund checks. Once approved, a final run is produced and an outsourced vendor file for disbursement processing is created.
 	
• The sequential numbering profile option for disbursements is enabled and in use to control the check numbers produced by the outsource vendor.
 	
• Hash totals are used for the payment, address and client information. Hash totals are produced during the initial run and compared to the final run. Any changes cause the processing of the outsource vendor file to abort and the error is written to a log for further review.
	• *Inspected* various QMS documentation including:
	   ▪ Refunds (Overpayments)
	   ▪ Reconciliations (Refunds, Voids)
	   ▪ Returned (Un-cashed Refund)
	   ▪ Reversing a Refund
	   ▪ Refund Invoices Inquiry
	   ▪ Manually Paying Refunds
	   ▪ Manually Voiding Refunds
	
	• *Obtained and tested* a sample set of refunds batched verifying they were processed according to the stated procedures.
	
	• *Inquired* of the Project Finance Director, Reconciliation and Refunds Supervisor for Financial Operations, and the Supervisor for Accounts Payable/Receivable as to policies and procedures set in place for Refund Output Controls.
		No relevant exceptions were noted. The documents inspected confirm management's description.
		
		No relevant exceptions were noted. The information reviewed confirms management's description.
		
		No relevant exceptions were noted. The inquiries confirm management's description.

IV. Oracle Financials – HFP and AIM - Application Controls – Input, Processing and Output		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
4. The Oracle Financials "Auto Invoice Process" will not run against all of the records in the open interface table creating customer invoices until a series of validations are completed.	• *Inquired* of the Financial Operations Director as to the process of invoicing output controls.	No relevant exceptions were noted. The inquiries confirm management's description. Noted that prior to the auto invoicing function a series of validation checks occurs including but not limited to a check for active participants, an amount to be billed, and credit before the invoice is generated and the file sent to KP Corp. If anyone fails the case goes to a carve-out file for further verification and a follow-up/corrected run is sent to KP Corp after the primary to provide for correction necessary.
5. Error handling procedures for output exist and are followed.	• *Reviewed* various QMS documentation including: ▪ Void Process for Returned Refund Checks ▪ Systems – Monitoring and Controls of Nonconforming Product • *Inquired* of the Supervisor for Accounts Payable/Receivable noting that carve-out files are produced with the errors and are reviewed.	No relevant exceptions were noted. The information reviewed confirms management's description. No relevant exceptions were noted. The inquiries confirm management's description.

IV. Oracle Financials – HFP and AIM - Application Controls – Input, Processing and Output		
Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
6. Activity Reporting / Monitoring includes: • Procedures for developing reports exist. • Routine reports are generated for monitoring output and performance.	• *Inquired* of the Project Finance Director and the Supervisor for Accounts Payable/Receivable regarding the procedures for developing reports as well as the frequency and generation of routine reports for monitoring the output and performance.	No relevant exceptions were noted. The inquiries confirm management's description.
	• *Reviewed* routine reports produced by the system noting conformity with stated policy.	No relevant exceptions were noted. The information reviewed confirms management's description.